Bezpieczeństwo systemów IT – Kraków, 24-25.09.2009r.

Program szkolenia

Dzień 1 (10:45-17:00)

10:15 - 10:45 -- Rejestracja
10:45 - 11:00 -- Powitanie. Przestawienie prelegenta oraz tematyki szkolenia
11:00 - 11:30 -- Elementy bezpieczeństwa informacji
- Poufność
- Integralność
- Dostępność
- Rozliczalność
- Przykłady naruszeń

11:30 - 11:45 Przerwa
11:45 - 12:45 Zarządzanie ryzykiem
- Zasoby
- Zagrożenia
- Analiza ryzyka
- Koszty zabezpieczeń vs. koszty strat

12:45 - 13:45 -- Obiad
14:00 - 15:30 -- Kryptografia - wybrane zagadnienia
- Cele stawiane kryptografii
- Kryptografia symetryczna i asymetryczna. DES, AES, RSA, ECC, DH. Tryby pracy algorytmów blokowych
- Funkcje hashujące oraz algorytmy MAC (Message Authentication Code) - HMAC, CBC-MAC
- Podpis cyfrowy. Certyfikaty cyfrowe
- Ogólne omówienie protokołu HTTPS - jako przykład kryptografii zapewniającej poufność, integralność oraz uwierzytelnianie stron
- Omówienie wybranych opcji oprogramowania openssl
- Praktyczny pokaz łamania wybranych szyfrów

15:30 - 15:45 -- Przerwa
15:45 - 17:00 -- Wybrane zagadnienia bezpieczeństwa warstwy sieciowej
- Wybrane topologie sieci
- Systemy IDS
- Fierwalle. Omówienie klas
- Standard 802.1X jako przykład kontroli dostępu do sieci. Omówienie funkcjonalności oferowanej przez RADIUS
- Przegląd wybranych zabezpieczeń warstwy 2 OSI
- IPsec jako przykład zabezpieczeń warstwy 3 OSI
- SSL jako przykład zabezpieczeń warstwy 4-5 OSI
- Firewall aplikacyjny jako przykład zabezpieczeń warstwy 7 OSI

Dzień 2 (9:00 - 16:00)

8:15 - 8:45 -- Śniadanie
8:45 - 9:00 -- Poranna kawa
9:00 - 10:15 -- Bezpieczeństwo systemów operacyjnych
- Usługi sieciowe
- Aktualizacje

- Przegląd wybranych dodatkowych zabezpieczeń oferowanych przez systemy operacyjne - jail, security levels, kernel hardening, umożliwienie dostępu w trybie innym niż klasyczny DAC -- RBAC, MAC
- Ogólny hardening

10:15 - 10:30 -- Przerwa
10:30 - 11:45 -- Bezpieczeństwo wybranych elementów oprogramowania infrastruktury
- Bazy danych
- Serwery aplikacyjne
- Serwery DNS
- Serwery HTTP

12:00 - 13:00 -- Obiad
13:15 - 14:45 -- Bezpieczeństwo aplikacji
- Najczęstsze klasy podatności
- Ogólne omówienie jednej z najbardziej znanych klasy podatności - buffer overflow
- Zabezpieczenia stosowane dla aplikacji
- Bezpieczeństwo WEB

14:45 - 15:00 -- Przerwa
15:00 - 15:45 -- Ataki na systemy IT
- Przykłady ataków warstwie sieciowej
- Przykłady ataków na systemy WWW
- Przykłady ataków hybrydowych. Prezentacja w czasie rzeczywistym realnego ataku tej klasy
- Przykłady ataków klasy social engineering
- Przykłady ataków fizycznych na systemy

15:45 - 16:00 -- Zakończenie szkolenia

Grupa docelowa

Szkolenie przeznaczone jest dla:
- Pracowników departamentów bezpieczeństwa firm
- Pracowników działów IT
- Osób odpowiedzialnych za wdrażanie zabezpieczeń w organizacjach
- Osób pragnących usystematyzować / poszerzyć swoją ogólną wiedzę z zakresu bezpieczeństwa IT

Prowadzący szkolenie

Michał Sajdak jest dyrektorem d/s rozwoju oraz konsultantem w firmie Securitum.

- Absolwent Uniwersytetu Jagiellońskiego (informatyka)
- Posiada wieloletnie doświadczenie w dziedzinach: bezpieczeństwa IT, tworzenia oprogramowania (głównie aplikacje dla instytucji finansowych) oraz administracji systemami
- Posiadacz certyfikatu CISSP (#338973)
- Wykonywał audyty bezpieczeństwa – w tym testy penetracyjne – dla największych organizacji w Polsce

Cena szkolenia

Cena szkolenia wynosi 2200 PLN netto / osobę i zawiera:
- Udział w seminarium

- Książka "Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses (2nd Edition)"

- Nocleg w hotelu trzygwiazdkowym (pokoje jednoosobowe)
- Dostępne w trakcie szkolenia: kawa, herbata, woda, soki, ciasteczka - bez limitu
- Wyżywienie (śniadanie, 2 x obiad, kolacja)
- Konspekt szkolenia

- Certyfikat ukończenia szkolenia

W przypadku uczestnictwa w szkoleniu dwóch lub większej ilości osób z jednej firmy - dla każdego kolejnego uczestnika udzielamy 20% rabatu.