Kod szkolenia: **SEC/INTRO**

Tytuł szkolenia: **Wprowadzenie do bezpieczeństwa informacji**

Dni: 1

Opis:

Adresaci szkolenia

Szkolenie przeznaczone jest dla osób pragnących zapoznać się z problematyką bezpieczeństwa informacji oraz technikami stosowanymi w tej dziedzinie. Dedykowane jest dla osób odpowiedzialnych za przygotowanie, wykonanie oraz wdrożenie projektów informatycznych od strony związanej z zarządzaniem oraz analizą i architekturą (kadra zarządzająca, architekci oprogramowania).

Cel szkolenia

Uczestnicy dowiedzą się jakie są współczesne zagrożenia dla systemów i danych, w jaki sposób szacuje się ryzyko związane z ich użytkowaniem i przetwarzaniem oraz jakimi technikami zwiększa się ich bezpieczeństwo.

Mocne strony szkolenia

Szkolenie ma charakter wykładowy z grą symulacyjną. Podczas szkolenia uczestnicy:

- zobaczą jak zagrożenia mogą wpłynąć na działalność i finanse organizacji,
- zrozumieją podstawowe techniki oraz cel szacowania ryzyka,
- dowiedzą się jakimi technikami zabezpiecza się sieci komputerowe oraz dane elektroniczne,
- podczas gry symulacyjnej oszacują ryzyko, przygotują plan ochrony organizacji i sprawdzą jego skuteczność dla przykładowych ataków i awarii.

Wymagania

Od uczestników wymagana jest ogólna wiedza z zakresu wykorzystania komputera w codziennej pracy i podstawowych pojęć z tym związanych.

Specjalne wymagania techniczne

Brak.

Parametry szkolenia

1 * 8 godzin (1 * 7 godzin netto) wykładów i warsztatów.

Program szkolenia:

1. Współczesne zagrożenia dla danych elektronicznych

    - czym jest bezpieczeństwo informacji
    - dlaczego należy chronić dane
    - wybrane skutki utraty kontroli nad danymi
    - pojęcie integralności, poufności i dostępności
    - wymagania dotyczące przetwarzania danych
    - wybrane ramy prawne związane z ochroną i zagrożeniami dla informacji: rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO), kodeks karny
    - wybrane zalecenia i standardy przemysłowe związane z ochroną informacji: przetwarzanie danych posiadaczy kart płatniczych (PCI DSS)
    - określanie poziomu bezpieczeństwa systemów informatycznych
    - hakerzy, crackerzy i *script-kiddies*, etyczny haking
    - złośliwe oprogramowanie, *malware* i wirusy komputerowe
    - ataki socjotechniczne, podszywanie się, *phishing*
    - programy antywirusowe, ochrona przed *malware*
    - kopie zapasowe

2. Szacowanie ryzyka

    - pojęcie ryzyka
    - analiza i ocena ryzyka, zarządzanie ryzykiem
    - cel procesu szacowania ryzyka
    - określanie aktywów, zagrożeń i podatności
    - kontrola fizyczna, administracyjna i techniczna
    - określanie wpływu zagrożeń oraz poziomu zabezpieczeń
    - szacowanie ryzyka a wycena projektu i jego architektura

3. Podstawy kryptografii

    - ochrona integralności, funkcje skrótu
    - szyfrowanie, wykorzystanie kluczy kryptograficznych
    - szyfr *nie do złamania* - 100% bezpieczeństwo a praktyka
    - problem wymiany klucza oraz zarządzania kluczami
    - techniki szyfrowania symetrycznego i asymetrycznego
    - najważniejsze współczesne algorytmy kryptograficzne: rodzina SHA (w tym

SHA-3), AES, 3DES, DH, RSA, algorytmy oparte o krzywe eliptyczne (ECDH, ECIES, ECDSA)
- problem autentyczności klucza publicznego

4. Identyfikacja i uwierzytelnienie

- pojęcie identyfikacji i uwierzytelnienia
- stosowanie haseł i fraz hasłowych
- karty elektroniczne i tokeny
- techniki biometryczne
- pojęcie podpisu cyfrowego
- certyfikat klucza publicznego i jego rola w infrastrukturze klucza publicznego (ang. *public key infrastructure*, PKI)
- zarządzanie tożsamością, usługi IDaaS (ang. *identity as a service*) i SSO (ang. *single sign-on*)

5. Bezpieczeństwo sieci komputerowych

- podstawy działania sieci komputerowej: architektura, adresacja, porty
- podstawowe usługi sieciowe, pojęcie sieci wewnętrznej i strefy zdemilitaryzowanej
- ściany ogniowe (ang. *firewall*)
- systemy wykrywania włamań (ang. *intrusion detection systems*, IDS)
- systemy zapobiegania włamaniom (ang. *intrusion prevention systems*, IPS)
- systemy honeypot
- testy penetracyjne sieci i usług sieciowych
- wirtualne sieci prywatne (ang. *virtual private networks*, VPN)
- protokoły SSL/TLS i IPsec
- bezpieczeństwo sieci i zasobów na przykładzie chmury obliczeniowej

6. Incydenty bezpieczeństwa

- podstępowanie w przypadku zaistnienia incydentu
- systemy SIEM (ang. *security information event management*)
- informatyka śledcza
- zbieranie dowodów
- odpowiedź na incydent
- incydent a katastrofa

7. Plan awaryjny

- pojęcie ciągłości działania

- opracowanie planu awaryjnego
- redundancja systemów i danych

Sages sp. z o.o., ul. Nowogrodzka 62c, 02-002 Warszawa
tel. +48 22 203 56 00 fax: +48 22 203 56 01
e-mail: biuro@sages.com.pl web: www.sages.com.pl