Security awareness. Bezpieczny pracownik w sieci

Omówienie

Celem szkolenia jest zwiększenie bezpieczeństwa organizacji poprzez podnoszenie poziomu kompetencji pracowników w zakresie bezpieczeństwa teleinformatycznego, w szczególności w zakresie ochrony danych, informacji i wiedzy na temat zagrożeń sieciowych oraz inżynierii społecznej – socjotechniki stosowanej w naruszeniach bezpieczeństwa sieci.

W ramach szkolenia omawiane są następujące obszary:

- Świadomość zagrożeń - rozumienia na jakie niebezpieczeństwa narażeni są pracownicy korzystający z komputerów, smartphone'ów i innych urządzeń i usług teleinformatycznych
- Umiejętności rozpoznawania zagrożeń i właściwego reagowania, w tym informowania o zdarzeniach i podejmowania decyzji w sposób przemyślany, zgodnie z zasadami bezpieczeństwa
- Bezpiecznego korzystania z nowoczesnych technologii w pracy i domu
- Obowiązku ochrony informacji i zabezpieczania środowiska pracy
- Odpowiedzialność za utrzymanie bezpieczeństwa informacji i reputacji instytucji oraz zaufania obywateli i klientów

Adresaci szkolenia

Proponowany program szkolenia dedykowany jest wszystkim osobom pracującym na co dzień z komputerem podpiętym do sieci LAN i Internetu. Uczestnik szkolenia dowie się jak wykrywać zagrożenia oraz jak prawidłowo na nie reagować.

Zakres tematyczny

1. Charakterystyka współczesnych zagrożeń bezpieczeństwa IT
2. Aspekt zarządzania bezpieczeństwem IT
3. Zagadnienia bezpieczeństwa w poszczególnych obszarach, takich jak: bezpieczeństwo fizyczne, organizacyjne, bezpieczeństwo informacji, polityki bezpieczeństwa, dobre praktyki stosowania zasad bezpieczeństwa
4. Rola procedur i świadomości użytkowników (dlaczego stosowanie się do zasad bezpieczeństwa jest ważne)
5. Konsekwencje nie stosowania się do zasad, procedur i dobrych praktyk
6. Straty na jakie organizacja jest narażona w przypadku zaistnienia incydentów naruszających bezpieczeństwo – reagowanie na zagrożenia.

W ramach poszczególnych obszarów, w trakcie szkolenia będą przedstawiane miedzy innymi takie zagadnienia jak:

Akademia NASK
ul. Kolska 12, 01-045 Warszawa
tel: +48 22 380 82 00, 380 85 49
szkolenia@nask.pl, www.akademia.nask.pl

Obszar zagrożeń:

1. Ty też jesteś celem. Ludzkie słabości i emocje – naturalne reakcje ludzkie w obliczu współczesnych zagrożeń.
2. Czym jest złośliwe oprogramowanie?
3. Bezpieczeństwo haseł (min. Bezpieczne i silne hasła, Systemy zarządzania hasłami, Dwustopniowe uwierzytelnianie)
4. Socjotechnika on-line , Phishing i Spear Phishing czyli oszustwa w e-mailach i mediach społecznościowych
5. Bezpieczeństwo i prywatność w przeglądarkach
6. Pracownik w podróży i praca zdalna.
7. Fałszywe strony
8. Oszustwa w bankowości internetowej

Dobre praktyki zabezpieczania:

1. Czym jest firewall, antywirus?
2. 5 kroków dla własnego bezpieczeństwa
3. Email – kilka prostych porad
4. Bezpieczny komputer w siedmiu krokach
5. Backup i przywracanie danych
6. Bezpieczne korzystanie z chmury
7. Aktualizowanie oprogramowania
8. Rozumienie wagi szyfrowania
9. Bezpieczne zakupy w sieci
10. Bezpieczeństwo w serwisach społecznościowych
11. Bezpieczeństwo w podróży
12. Bezpieczne urządzenia i aplikacje mobilne
13. Bezpieczeństwo sieci WiFi

Czas trwania

Moduł szkoleniowy (4-godziny) zakończony krótkim podsumowaniem i testem dla uczestników szkolenia.

Prowadzący

Eksperci Zespołu Menadżerów Produktów NASK.

Akademia NASK
ul. Kolska 12, 01-045 Warszawa
tel: +48 22 380 82 00, 380 85 49
szkolenia@nask.pl, www.akademia.nask.pl