Ochrona danych

SZKOLENIE PRAKTYCZNE

DLA STUDENTÓW POLITECHNIKI CZĘSTOCHOWSKIEJ

Plan szkolenia

- Czym są dane?
- Co to jest ochrona danych?
- Jakie zagrożenia na mnie czyhają?
- Dobre praktyki
- Podsumowanie

Czym są dane?

- Wszystkie informacje jakie przetwarzamy są danymi objętymi ochroną
- Szczególny typ danych stanowią dane osobowe
- Dane mogą być przetwarzane metodami tradycyjnymi, czyli papierowo, a także elektronicznie

Dane osobowe

- Definiuje się je jako informacje, dzięki którym możliwe jest zidentyfikowanie osoby fizycznej. Są to wszystkie informacje o osobie, której tożsamość jest oczywista lub jej zidentyfikowanie nie wymaga wielkiego nakładu pracy, czasu czy kosztów, tak jak podaje ustawa.
- Oznacza to, że osoba ta nie musi być wskazana bezpośrednio - wystarczy nam zbiór informacji, które pozwolą bezpośrednio lub pośrednio daną osobę zidentyfikować, np. e-mail z imieniem i nazwiskiem w domenie firmy, przykładowo pcz.pl.

Co to jest ochrona danych?

- Ochrona danych, to przede wszystkim zdroworozsądkowe i racjonalne postępowanie z powierzoną nam informacją.
- Informację, którą posiadamy lub przetwarzamy musimy chronić przed nieumyślnym uszkodzeniem, zniszczeniem, ujawnieniem, wykradzeniem lub inną formą utraty.
- Zniszczenie, uszkodzenie lub ujawnienie danych jest prawnie zakazane i podlega odpowiedzialności karnej.

Jakie zagrożenia na mnie czyhają?

- Najczęstsze zagrożenia dla danych, jakie mogą nas spotkać w codziennym życiu, to m.in.:
- Złamanie lub ujawnienie hasła
- Próby wyłudzenia danych i dostępu do systemu, tzw. phishing
- Działanie szkodliwego oprogramowania (wirusy, trojany, ransomware)
- Przypadkowe ujawnienie, uszkodzenie lub skasowanie danych

Dobre praktyki

- Hasła, pod żadnym pozorem, nie wolno nikomu ujawniać, ani zapisywać w jawnej formie
- Administratorzy systemów nigdy nie poproszą Cię o hasło!
- Używane w systemach hasło nie może być proste do odgadnięcia i nie powinno być słownikowe (np. składać się z wyrazu, imienia i cyfry)
- Zmieniaj regularnie hasła w systemach. Kolejne hasło musi się różnić co najmniej kilkoma znakami od poprzedniego
- Jeżeli masz podejrzenie ujawnienia hasła – natychmiast je zmień
- Dbaj o swoje hasło, jak o PIN do karty bankomatowej!

Dobre praktyki

- Na komputerze musisz mieć zainstalowany aktualny program antywirusowy
- Skanuj komputer co najmniej raz w tygodniu
- Nie pobieraj z Internetu podejrzanych plików
- Szczególnie uważaj na podejrzane e-maile

Dobre praktyki

- Przestępcy są bardzo przebiegli i potrafią podszywać się pod znane Ci osoby
- Nigdy ślepo nie ufaj rozmówcy lub e-mailom, które otrzymujesz
- Nie otwieraj podejrzanych załączników
- Nie klikaj w linki w e-mailach
- Zawsze sprawdzaj, czy wiadomość została wysłana od osoby, którą znasz
- Administratorzy systemów NIGDY nie poproszą Cię o Twoje hasło – to najczęstsza próba wyłudzenia hasła.
- Nigdy nie przekazuj loginów i haseł przez telefon, e-mail, komunikator internetowy

Podsumowanie

- Dbaj o swój login i hasło, bo to one potwierdzają Twoją tożsamość
- Nigdy nie ujawniaj swojego hasła
- Administratorzy systemów nie potrzebują Twojego hasła, więc każda informacja z prośbą o jego podanie, bądź z linkiem do logowania, jest próbą oszustwa
- Niezwłocznie zgłaszaj podejrzenia złamania hasła lub inne nieprawidłowości