Uczelniane Centrum Informatyczne

Ochrona danych

Szkolenie praktyczne dla pracowników Politechniki Częstochowskiej

Uczelniane Centrum Informatyczne, kwiecień 2019 r.

Uczelniane Centrum Informatyczne

Plan szkolenia

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

Uczelniane Centrum Informatyczne

Czym są dane i tajemnica przedsiębiorstwa

- Wszystkie informacje jakie przetwarzamy są danymi objętymi ochroną
- Szczególny typ danych stanowią dane osobowe
- Tajemnica przedsiębiorstwa, to tzw. know-how, czyli dobra intelektualne wytworzone i opracowane na Politechnice
- Dane mogą być przetwarzane metodami tradycyjnymi, czyli papierowo, a także elektronicznie

Uczelniane Centrum Informatyczne

Czym są dane i tajemnica przedsiębiorstwa

Wszystkie informacje jakie przetwarzamy są danymi objętymi ochroną. Są to wszelkiego rodzaju dokumenty i pliki zawierające informacje o osobach lub instytucji. Do danych zaliczamy:

- Dane osobowe
- Tajemnicę przedsiębiorstwa

Uczelniane Centrum Informatyczne

Czym są dane i tajemnica przedsiębiorstwa

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.

Uczelniane Centrum Informatyczne

Czym są dane i tajemnica przedsiębiorstwa

Tajemnica przedsiębiorstwa

Objęte ochroną ustawową są informacje o bardzo różnym charakterze – zarówno techniczne i technologiczne, ale też związane ze sposobem funkcjonowania przedsiębiorstwa i jego organizacją. Wśród informacji będących tajemnicą przedsiębiorstwa można wskazać np. oferty przetargowe, aktywa i pasywa oferentów, dochód i zyski, koszty działalności, straty, zobowiązania finansowe, wielkość sprzedaży, źródła zaopatrzenia, dane kontrahentów, plany rozwoju.

Uczelniane Centrum Informatyczne

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.

Uczelniane Centrum Informatyczne

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
- Uszkodzenie sprzętu, a w konsekwencji utrata danych
- Ujawnienie lub uszkodzenie dokumentacji papierowej
- Używanie prywatnych urządzeń do celów służbowych
- Używanie służbowych urządzeń do celów prywatnych

Uczelniane Centrum Informatyczne

Dobre praktyki

Dobre praktyki, to zbiór zasad i wskazówek, jak postępować w określonych sytuacjach w celu uniknięcia naruszenia danych, które przetwarzamy.

Dobre praktyki - hasło

Uczelniane Centrum Informatyczne

Pamiętaj!

- 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!

Uczelniane Centrum Informatyczne

Dobre praktyki – ochrona plików

Pamiętaj:

- Na komputerze musisz mieć zainstalowany aktualny program antywirusowy
- Skanuj komputer co najmniej raz w tygodniu
- Nie korzystaj z prywatnych pendrivów i dysków zewnętrznych
- Przy każdym podłączeniu elektronicznego nośnika zewnętrznego przeskanuj go na obecność zagrożeń
- Nie instaluj samodzielnie żadnego oprogramowania
- Nie pobieraj z Internetu podejrzanych plików
- Szczególnie uważaj na podejrzane e-maile

Dobre praktyki – phishing

Uczelniane Centrum Informatyczne

Pamiętaj:

- 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
- W razie wątpliwości, zawsze skontaktuj się z pracownikami UCI
- Wszelkie próby wyłudzeń zgłaszaj przełożonemu i do UCI
- Przeprowadź krótki test, czy rozumiesz te zagrożenia https://phishingquiz.withgoogle.com

Uczelniane Centrum Informatyczne

Dobre praktyki – archiwizacja

Pamiętaj:

- Masz obowiązek zabezpieczyć przetwarzane dokumenty przed ich utratą
- Nie pracuj na pendrivie. To bardzo zawodne urządzenie i służy jedynie do przenoszenia plików.
- Docelowo, każdy pracownik Uczelni otrzyma przestrzeń w prywatnej chmurze PCz
- Pracownicy UCI zawsze pomogą w wyborze sposobu i zakresu archiwizacji

Uczelniane Centrum Informatyczne

Dobre praktyki – szyfrowanie plików

Pamiętaj:

- Masz obowiązek zabezpieczyć przetwarzane dokumenty przed nieuprawnionym dostępem osób trzecich
- Jeżeli wysyłasz lub wynosisz dane poza Politechnikę, powinieneś zabezpieczyć je za pomocą szyfrowania
- Jeżeli posiadasz zgodę na wynoszenie laptopów służbowych poza Uczelnię, to ich dyski muszą być odpowiednio zabezpieczone
- Do szyfrowania używaj mocnych i złożonych haseł

Uczelniane Centrum Informatyczne

Dobre praktyki – zabezpieczenia fizyczne

Pamiętaj:

- Pracując poza Uczelnią, musisz zadbać o odpowiednie środowisko pracy
- Zwróć uwagę, czy ktoś nie czyta Ci „przez ramię”
- Nie podłączaj się do nieznanych sieci WiFi
- Nie udostępniaj nikomu komputera i / lub komórki służbowej
- Zadbaj o to, żeby ktoś nie przechwycił Twoich wydruków
- Nie loguj się swoimi danymi na nieznanych komputerach, np. w hotelach itp.
- Jeżeli potrzebujesz połączyć się z PCz spoza sieci uczelnianej, korzystaj z bezpiecznego połączenia VPN

Uczelniane Centrum Informatyczne

Dobre praktyki – zabezpieczenia fizyczne cd.

Pamiętaj:

- W momencie odejścia od biurka, zabierz ze sobą lub schowaj dokumenty, zawierające dane podlegające ochronie i obowiązkowo zablokuj komputer
- Wychodząc, nigdy nie pozostawiaj niezamkniętego pokoju
- Pod żadnym pozorem nie wolno pozostawiać w pomieszczeniach służbowych osób trzecich bez nadzoru
- Stosuj zasadę czystego biurka i pulpitu w komputerze – nie zapisuj dokumentów na pulpicie
- Trzymaj na biurku/ekranie tylko te dokumenty, na których aktualnie pracujesz

Uczelniane Centrum Informatyczne

Dobre praktyki – zabezpieczenia fizyczne cd.

Pamiętaj:

- Ochrona danych polega również na zabezpieczeniu ich przed przypadkowym skasowaniem, uszkodzeniem, całkowitym lub częściowym zniszczeniem
- W związku z tym, zadbaj o stan swojego komputera – wszelkie nieprawidłowości w działaniu zgłaszaj do UCI
- Kluczowe komputery powinny być zabezpieczone przed utratą zasilania
- Pracując na dokumentach papierowych, dbaj o nie. Uważaj, żeby ich nie zalać, uszkodzić lub przez przypadek nie zniszczyć
- Kseruj i drukuj dokumenty tylko na zaufanych, służbowych urządzeniach
- Do niszczenia dokumentów zawierających dane chronione, używaj niszczarek

Uczelniane Centrum Informatyczne

Dobre praktyki – systemy informatyczne

- Dbaj o aktualność systemu operacyjnego – pozwól systemowi zaktualizować się
- Regularnie, nie rzadziej niż co 3 dni, restartuj komputer
- Pamiętaj o wyrzuceniu skasowanych dokumentów z kosza
- Nie używaj tych samych haseł do spraw służbowych i prywatnych
- Nie łącz się z miejsca pracy z witrynami i serwerami mogącymi nieść ze sobą ryzyko infekcji szkodliwym oprogramowaniem (np. pobieranie muzyki, itp.)
- Nie modyfikuj i nie zmieniaj zainstalowanego przez administratorów systemu aplikacji
- Wszelkie podejrzane zachowania i sytuacje niezwłocznie zgłaszaj przełożonym
- Nie wykorzystuj do celów służbowych sprzętu prywatnego
- Nie używaj służbowego komputera do celów prywatnych
- Przed oddaniem komputera do serwisu skontaktuj się z UCI – razem z komputerem możesz przypadkowo udostępnić dane

Uczelniane Centrum Informatyczne

Ochrona danych - podsumowanie

- Podczas pracy nad dokumentami podlegającymi ochronie zachowaj szczególną staranność i ostrożność
- W kontaktach telefonicznych, cyfrowych, jak również osobistych z nieznanymi osobami, zachowaj zasadę ograniczonego zaufania
- 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