POLITECHNIKA Politechnika Częstochowska

[UCI]

Bezpieczeństwo informacji w systemach teleinformatycznych

Szkolenie dla pracowników Politechniki

Plan szkolenia

1. Czym są dane i tajemnica przedsiębiorstwa?
2. Co to jest ochrona danych?
3. Jakie zagrożenia na mnie czyhają?
4. Dobre praktyki
5. Skutki naruszenia zasad bezpieczeństwa
6. Podsumowanie

1. 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 w Politechnice Częstochowskiej.
- Dane mogą być przetwarzane metodami tradycyjnymi, czyli papierowo, a także elektronicznie.

Przetwarzane dane objęto ochroną są to wszelkiego rodzaju dokumenty i pliki zawierające informacje o osobach lub instytucji. Do danych zaliczamy:

- dane osobowe,
- tajemnicę 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*.

Tajemnica przedsiębiorstwa

Tajemnica przedsiębiorstwa to tzw. *know-how*, czyli dobra intelektualne wytworzone i opracowane na Politechnice. 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, dane kontrahentów czy plany rozwoju.

2. 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.

3. 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 (np. wirusy, konie trojańskie, *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.

4. Dobre praktyki

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

Hasło użytkownika

- 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!

Ochrona plików

- Na komputerze musisz mieć zainstalowany aktualny program antywirusowy.
- Skanuj komputer co najmniej raz w tygodniu.
- Nie korzystaj z prywatnych pendrive'ów 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.**

Phishing

- 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

Archiwizacja

- Masz obowiązek zabezpieczyć przetwarzane dokumenty przed ich utratą.
- Nie pracuj na pendrive. To bardzo zawodne urządzenie i służy jedynie do przenoszenia plików.
- Pracownicy UCI zawsze pomogą w wyborze sposobu i zakresu archiwizacji.

Szyfrowanie plików

- 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.

Zabezpieczenia fizyczne

- 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.**
- 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.
- 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.

Systemy informatyczne

- Dbaj o aktualność systemu operacyjnego – pozwól systemowi zaktualizować się na bieżąco.
- Regularnie, 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, hazard itp.).
- Nie modyfikuj i nie zmieniaj zainstalowanego przez administratorów systemu i 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.

5. Skutki naruszenia zasad bezpieczeństwa

Skutki dla Uczelni

Prócz odpowiedzialności prawnej, która jest istotnym następstwem naruszeń zasad bezpieczeństwa informacji w systemach teleinformatycznych, należy nadmienić, iż równie istotne są skutki wynikające z niewłaściwego – celowego lub nie – wykorzystania systemów informatycznych prowadzącego do wycieku lub zniszczenia danych.

Z punktu widzenia funkcjonowania Uczelni zniszczenie danych w systemach informatycznych, np. klasy ERP może prowadzić do częściowego paraliżu w funkcjonowaniu istotnych dla każdego przedsiębiorstwa obszarach. Wykonywanie pracy w niewłaściwy sposób może doprowadzić do niemożności realizacji podstawowych celów jednostek, w tym wymaganych przez podmioty zewnętrzne, co obwarowane może być karami finansowymi nakładanymi na Uczelnie. To samo tyczy się wycieku ważnych informacji (w kontekście obowiązującego tzw. RODO).

Każdy pracownik musi mieć na uwadze, że jeżeli bezpośrednio przyczyni się swoimi działaniami do problemów pracodawcy, ma on prawo prowadzić działania prowadzące do rekompensaty swoich strat na drodze sądowej, co skutkować może nałożeniem grzywny/kary finansowej na pracownika lub w szczególnych przypadkach ograniczeniem/pozbawieniem wolności.

Odpowiedzialność prawna

Kodeks pracy

W zależności od okoliczności sytuacji dotyczącej naruszenia zasad bezpieczeństwa, najczęstszymi konsekwencjami są:

- **upomnienie pracownika,**
- **rozwiązanie umowy za wypowiedzeniem,**
- **rozwiązanie umowy bez wypowiedzenia** – z winy pracownika (w przypadku rażącego naruszenia podstawowych obowiązków pracowniczych).

Zgodnie z Kodeksem Pracy, **pracownik który na skutek niewykonania lub nienależytego wykonania obowiązków pracowniczych**, ze swojej winy, wyrządził pracodawcy szkodę, **ponosi odpowiedzialność materialną** w granicach rzeczywistej straty poniesionej przez pracodawcę. Wówczas odszkodowanie ustala się w wysokości wyrządzonej szkody, jednak nie może ono przewyższać kwoty trzymiesięcznego wynagrodzenia pracownika w dniu wyrządzenia szkody.

Kodeks karny

Kodeks karny przewiduje określone kary w związku z przestępstwami przeciwko ochronie informacji:

- **Ujawnianie lub wykorzystanie informacji niejawnych** o klauzuli „tajne" lub „ściśle tajne" podlega karze pozbawienia wolności od 3 miesięcy do 5 lat, a w przypadku gdy ujawniono informacje na rzecz podmiotu zagranicznego, od 6 miesięcy do 8 lat. W przypadku gdy informacja została ujawniona nieumyślnie przez osobę w związku z pełnieniem funkcji lub publicznej lub otrzymanym upoważnieniem podlega grzywnie lub karze ograniczenia/pozbawienia wolności do roku.

- **Ujawnianie informacji w związku z wykonywaną funkcją** podlega grzywnie lub karze ograniczenia/pozbawienia wolności do lat 2.
- **Bezprawne uzyskanie informacji** przez osobę nieuprawnioną poprzez otwarcie zamknięte pisma, podłączenie się do sieci telekomunikacyjnej lub ominięcie elektronicznych/magnetycznych/informatycznych zabezpieczeń podlega grzywnie, karze ograniczenia/pozbawienia wolności do lat 2. Dotyczy to również uzyskania nieuprawnionego dostępu do systemu informatycznego, posługiwania się urządzeniem podsłuchowym/wizualnym.
- **Utrudnianie zapoznania się z informacją** poprzez zniszczenie, uszkodzenie lub usunięcie istotnej informacji (np. na nośniku informatycznym) w zależności od stopnia szkody podlega karze pozbawienia wolności od miesięcy do 5 lat.
- **Niszczenie danych informatycznych oraz zakłócanie systemów komputerowych** poprzez uszkodzenia spowodowane m.in. usuwaniem, zmienianiem danych informatycznych, które w istotny sposób zakłócają lub uniemożliwiają automatyczne przetwarzanie, gromadzenie/przekazywanie takich danych podlega karze pozbawienia wolności do lat 3. Osoby niebędące do tego uprawnione, które poprzez transmisję, zniszczenie, usunięcie, uszkodzenie w istotny sposób zakłócą pracę systemu informatycznego/teleinformatycznego lub sieci teleinformatycznej podlegają karze pozbawienia wolności od 3 miesięcy do 5 lat.

Ustawa o Ochronie Danych Osobowych

Zgodnie z Ustawą o Ochronie Danych Osobowych osoby przetwarzające dane osobowe bez stosownego uprawnienia podlegają grzywnie, karze ograniczenia/pozbawienia wolności do lat dwóch.

Kierowniku jednostki, pamiętaj o upoważnieniach do przetwarzania danych wystawianych przez Biuro Ochrony Danych, Informacji Niejawnych i Bezpieczeństwa lub o aktualnie obowiązującej podstawie prawnej, na podstawie której przetwarzane są dane osobowe w Twojej jednostce.

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.
- Pamiętaj o ewentualnych skutkach, w tym natury prawnej, naruszenia zasad bezpieczeństwa.

Zewnętrzne źródła informacji:

1) *Kodeks Karny (Dz.U.2022.1138 t.j. z dnia 2022.05.30)*
2) *Ustawa o Ochronie Danych Osobowych (Dz.U.2019.1781 t.j. z dnia 2019.09.19)*
3) *Kodeks Pracy (Dz.U.2022.1510 t.j. z dnia 2022.07.19)*

Polecamy artykuły, poradniki oraz informacje o zagrożeniach:

https://cert.orange.pl/

POLI
[TECH〉
NIKA

Politechnika
Częstochowska