KWARTALNIK

RODO

kwiecień 2024 **2/2024**

Ośrodek Pomocy Społecznej w Radzionkowie

Święta, święta i po świętach... Tym wydaniem witamy już w drugim kwartale roku 2024! Oby był równie owocny, jak poprzedni.

Co nowego w zakresie ochrony danych osobowych? Przede wszystkim fakt, iż w ramach realizacji Programu "Asystent osobisty osoby z niepełnosprawnością" dla Jednostek Samorządu Terytorialnego - edycja 2024 zatrudniliśmy w naszym Ośrodku 32 osoby, czym nadaliśmy upoważnienia do przetwarzania danych osobowych dla trzydziestu dwóch zleceniobiorców. Wszystkie osoby zostały przeszkolone w tym zakresie, a my jesteśmy pełni optymizmu odnośnie dalszej współpracy z zatrudnionymi osobami.

KWARTALNIK

RODO

kwiecień 2024 **2/2024**

Co w Biuletynie Urzędu Ochrony Danych Osobowych może nas wszystkich interesować?

PUBLICZNE ŁADOWANIE TELEFONU – RYZYKO CZY WYGODA?

W dzisiejszym świecie, gdzie nasze życie zawodowe i prywatne jest ściśle związane z urządzeniami elektronicznymi, korzystanie z publicznych portów USB może prowadzić do niebezpiecznych konsekwencji. Ładowanie telefonu czy tabletu, choć wydaje się być niegroźnym działaniem, może zostać wykorzystanie przez cyberprzestępców do ingerencji w system operacyjny urządzenia. Jednym z takich zagrożeń jest tzw. „juice jacking", który w ostatnich latach stał się coraz bardziej rozpowszechniony.

Juice jacking to szczególnie podstępny atak wykorzystujący naturalną potrzebę ładowania urządzenia poprzez podłączenie do publicznego, zewnętrznego źródła zasilania. Realizowany jest w taki sposób, że osoby atakujące modyfikują fabryczne ładowarki USB poprzez zainstalowanie dodatkowego modułu sprzętowego, co może doprowadzić do kradzieży danych lub zainstalowania złośliwego oprogramowania na urządzeniu użytkownika.

Publiczne porty USB, znajdujące się na lotniskach, w centrach handlowych, hotelach, kawiarniach czy w środkach transportu publicznego, mogą stać się

RODO

kwiecień 2024 **2/2024**

miejscami potencjalnych ataków na nasze urządzenia. Oto kilka zagrożeń:

• Kradzież danych: Atakujący mogą wykorzystać juice jacking do kradzieży danych przechowywanych na urządzeniu, takich jak kontakty, pliki, hasła itp.

• Zainstalowanie złośliwego oprogramowania: Poprzez zainfekowanie urządzenia złośliwym oprogramowaniem, atakujący mogą uzyskać zdalny dostęp do urządzenia lub zgromadzić poufne informacje.

• Ransomware: Atakujący mogą zainstalować ransomware na urządzeniu, co prowadzi do zablokowania dostępu do danych na urządzeniu i żądania okupu za ich odblokowanie.

• Podsłuchiwanie aktywności: Atakujący mogą wykorzystać juice jacking do podsłuchiwania aktywności użytkownika na zainfekowanym urządzeniu, co może prowadzić do kradzieży poufnych informacji.

Istnieją jednak sposoby ochrony przed takim atakiem, które mogą pomóc użytkownikom zminimalizować ryzyko kradzieży danych podczas ładowania urządzeń mobilnych.

Dzięki odpowiednim środkom ostrożności można zabezpieczyć się przed tego rodzaju zagrożeniami.

RODO

kwiecień 2024 **2/2024**

Co zatem należałoby zrobić, żeby nie paść ofiarą juice jackingu?

1. Przede wszystkim staraj się unikać korzystania z publicznych portów USB do ładowania urządzeń.
2. W razie konieczności korzystania z publicznych portów USB, należy pamiętać, żeby upewnić się, że nie mamy uruchomionego trybu „debugowanie USB", gdyż może to stanowić potencjalne zagrożenie dla bezpieczeństwa danych, ponieważ umożliwia dostęp do zaawansowanych funkcji urządzenia. Dlatego zaleca się wyłączenie tej opcji, co pozwoli na zminimalizowanie ryzyka nieautoryzowanego dostępu do urządzenia.
3. Alternatywnie, można korzystać z zewnętrznych baterii przenośnych do ładowania urządzeń lub kabli „only charge", które są przeznaczone wyłącznie do ładowania urządzenia i uniemożliwiają przesyłanie danych.
4. Zaleca się również regularnie sprawdzanie i instalowanie dostępnych aktualizacji systemu operacyjnego, aby zapewnić ochronę przed różnymi rodzajami ataków oraz utrzymać urządzenie w jak najbezpieczniejszym stanie.
5. Warto również zadbać o wyłączenie funkcji udostępniania danych na urządzeniu, gdy korzystamy z publicznych portów USB, aby ograniczyć ryzyko kradzieży danych. Ta prosta czynność może stanowić dodatkową warstwę ochrony dla użytkowników, którzy nie posiadają baterii przenośnych.
6. Ochronę urządzeń przed wirusami lub nieautoryzowanym pobraniem danych może zapewnić również tzw. bloker danych USB.

RODO

kwiecień 2024 **2/2024**

Może być skuteczną formą ochrony nie tylko w przypadku juice jacking, ale również ataków typu badUSB (np. przy wykorzystaniu specjalnie spreparowanych pendrive'ów), zapobiegając podłączeniu zainfekowanego urządzenia do komputera, ograniczając w ten sposób ryzyko zainfekowania. Publiczne porty USB mogą stanowić poważne zagrożenie dla bezpieczeństwa naszych danych i urządzeń, jednak świadomość tych zagrożeń oraz stosowanie odpowiednich środków ostrożności, takich jak unikanie publicznych portów USB i korzystanie z zabezpieczeń fizycznych, jest kluczowe dla ochrony naszych danych.

ZASADY PRACY Z DOKUMENTAMI ZAWIERAJĄCYMI DANE OSOBOWE

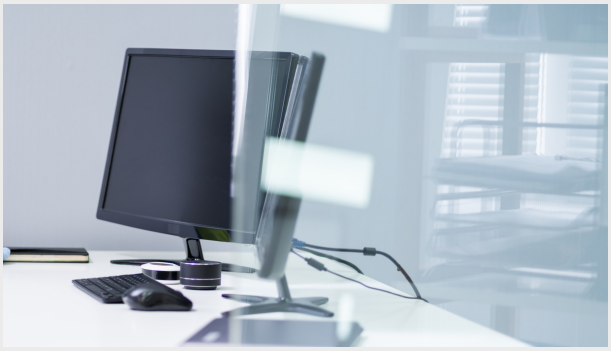
Za wszelkie dokumenty zawierające dane osobowe odpowiada pracownik, któremu te dokumenty zostały przekazane lub który sporządza dokumentację zawierającą dane, do momentu ich dalszego przekazania. W trakcie pracy z dokumentami obowiązuje "zasada czystego biurka", a tym samym:

- należy unikać pozostawiania dokumentów na biurku bez nadzoru, szczególnie, gdy dokumenty zawierają istotne z punktu widzenia Ośrodka Pomocy Społecznej w Radzionkowie dane;
- po zakończeniu pracy, wszystkie dokumenty mogące stanowić tajemnicę i zawierające dane osobowe, muszą być przechowywane w

RODO

kwiecień 2024 **2/2024**

zamknięciu i nie powinny być eksponowane w miejscu dostępnym.



W przypadku pracy na dokumentach, należy pamiętać, iż powinny być niszczone w sposób uniemożliwiający ich ponowne odczytanie, np. w niszczarce, umieszczane w specjalnie przeznaczonych do tego celu pojemnikach lub zutylizowane w sposób uniemożliwiający odczytanie.

Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych i ogólnodostępnych. Przy drukowaniu dokumentów z użyciem ogólnodostępnych drukarek, wszelkie drukowane informacje powinny być zabierane z drukarek niezwłocznie po wydrukowaniu. W przypadku prowadzenia prac z użyciem materiałów innych niż dokumenty, należy pamiętać, że po zakończonej pracy/spotkaniu należy uprzątnąć wszystkie materiały oraz wyczyścić nośniki informacji, np.: tablice, flipchart, etc.

Wynoszenie dokumentów poza siedzibę Ośrodka Pomocy Społecznej w Radzionkowie wymaga zaistnienia wyjątkowych okoliczności i uzyskania wyraźnej zgody Administratora danych.

RODO

kwiecień 2024 **2/2024**

W takich przypadkach, całkowita odpowiedzialność za zabezpieczenie danych osobowych spoczywa na pracowniku.

Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w teczkach. Osoba przewożąca dokumenty zobowiązana jest do zabezpieczenia przewożonych dokumentów przed zgubieniem i kradzieżą.

Jeśli dokumenty zostaną zgubione lub skradzione, należy ten fakt natychmiast zgłosić Administratorowi danych, wskazując jednocześnie, jakiego rodzaju dane były w tych dokumentach zawarte.

Osoby nieupoważnione nie mogą przenosić żadnych dokumentów zawierających dane.

Przekazywanie dokumentów zawierających dane osobowe odbywa się tylko i wyłącznie do rąk własnych osoby, której dane dotyczą lub upoważnionej przez nią osoby. Upoważnienie osoby powinno mieć formę pisemną.

KWARTALNIK

RODO

kwiecień 2024 **2/2024**

QUIZ - SZYBKIE STRZAŁY

1Należy dokonać zgłoszenia naruszenia do Urzędu Ochrony Danych Osobowych:

a. z zasady w ciągu 72 h od jego stwierdzenia

b. tylko pod groźbą tortur i to dopiero po drugim paznokciu

c. jeśli sprawa jest w procesie i walczymy już tylko o honor

d. zawsze, Prezes Urzędu jest jak Monika Olejnik - powinien wiedzieć wszystko

2.Działania korekcyjne i prewencyjne:

a. mają za zadanie minimalizować skutki naruszenia i zapobiec jego powtórzeniu

b. to przede wszystkim widowiskowy i uczciwy proces winnych, a także spektakularna ich egzekucja

c. przeprowadzamy, gdyż należy je wskazać w zgłoszeniu do UODO

d. nic nie pomogą, ludzie i tak się nie nauczą ...

3.Naruszenie poufności danych może polegać na:

a. przypadkowej zmianie informacji w koszykach zakupowych klientów sklepu internetowego

b. czasowej niedostępności części zbioru danych dla administratora

c. bezprawnym usunięciu części zbioru danych przez podmiot przetwarzający

d. przypadkowym opublikowaniu opisu życia osobistego współpracowników w intranecie organizacji

4.Administrator jest zobowiązany:

a. dokumentować naruszenie, o ile jest ono ciekawsze od trzeciego sezonu Wiedźmina

b. nic nie piszemy - przecież nie zostawiamy śladów!

c. dokumentować wszelkie naruszenia ochrony danych osobowych, w tym okoliczności ich wystąpienia, skutki oraz podjęte działania zaradcze

d. dokumentować naruszenie, jeżli dotyczyło naszych współpracowników a zbliża się czas podziału okresowych premii

1.a., 2.-a., 3.-d., 4.-c.