|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Nazwa procesu(krok 1)** | **Zaangażowane zasoby(krok 2)** | **Czyfirmowe?(krok 2)** | **Stosowane zabezpieczenia(krok 3)** | **Zagrożenia(krok 4)** | **Podatności(krok 5)** | **Waga(krok 6)** | **Prawdopodobieństwo(krok 6)** | **Ryzyko** |
| Obsługa klienta | Laptopy | NIE | * legalny system operacyjny i aplikacje mające wsparcie producenta,
* mechanizmy kontroli dostępu (login + hasło) znane jedynie użytkownikowi,
* wygaszacz ekranu chroniony hasłem,
* szyfrowanie dysku twardego.
 | * przypadkowe lub niezgodne z prawem zniszczenie danych osobowych,
* przypadkowa lub niezgodna z prawem utrata danych osobowych,
* przypadkowa lub niezgodna z prawem modyfikacja danych osobowych
* nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych.
 | * brak nadzoru nad sprzętem komputerowym,
* współdzielenie sprzętu komputerowego z wieloma osobami,
* ujawnienie osobom trzecim danych uwierzytelniających,
* uprawnienia administracyjne,
* wrażliwość na pył, wilgoć, temperaturę.
 | 1–4 | 1–4 |  |
| Lokalizacja zewnętrzna (mieszkania pracowników) | NIE | * miejsce wykonywania obowiązków ograniczające osobom postronnym możliwość wglądu w treść informacji,
* przechowywanie dokumentów papierowych w meblach zamykanych na klucz,
* rozmowy telefoniczne i konferencje prowadzone w pomieszczeniach gwarantujących poufność wymienianych informacji.
 | * przypadkowe lub niezgodne z prawem zniszczenie danych osobowych,
* przypadkowa lub niezgodna z prawem utrata danych osobowych,
* przypadkowa lub niezgodna z prawem modyfikacja danych osobowych,
* nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych.
 | * niewystarczająca kontrola dostępu,
* niestabilna sieć energetyczna,
* brak niezbędnej infrastruktury służącej do przetwarzania danych (meble, niszczarki).
 | 1–4 | 1–4 |  |
| Użytkownicy | TAK | * szkolenia z zakresu pracy zdalnej,
* upoważnienie do przetwarzania danych osobowych,
* procedura pracy zdalnej,
* procedura oraz ustanowione kanały komunikacji w razie kłopotów technicznych lub naruszenia ochrony danych osobowych.
 | * przypadkowe lub niezgodne z prawem zniszczenie danych osobowych,
* przypadkowa lub niezgodna z prawem utrata danych osobowych,
* przypadkowa lub niezgodna z prawem modyfikacja danych osobowych,
* nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych.
 | * niewystarczające szkolenie z zakresu bezpieczeństwa danych osobowych lub jego brak,
* niepoprawne użycie oprogramowania lub sprzętu,
* socjotechnika (m.in. phishing),
* brak świadomości w zakresie bezpieczeństwa,
* brak niezbędnych polityk w zakresie pracy zdalnej,
* frustracja pracowników (m.in. z powodu planowanego zwolnienia).
 | 1–4 | 1–4 |  |

Załącznik do artykułu: [Analiza ryzyka dla operacji przetwarzania realizowanych zdalnie](https://odo24.pl/blog-post.analiza-ryzyka-dla-operacji-przetwarzania-realizowanych-zdalnie)

Finalny poziom ryzyka stanowi iloczyn wagi zagrożenia oraz jego prawdopodobieństwa dla danego zasobu biorącego udział w operacji przetwarzania.
Możliwe kombinacje wskazanych wartości przedstawia poniższa tabela.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Waga** | **Bardzo wysoka (4)** | **4** | **8** | **12** | **16** |
| **Wysoka (3)** | **3** | **6** | **9** | **12** |
| **Średnia (2)** | **2** | **4** | **6** | **8** |
| **Niska (1)** | **1** | **2** | **3** | **4** |
|  | **Niskie (1)** | **Średnie (2)** | **Wysokie (3)** | **Bardzo wysokie (4)** |
| **Prawdopodobieństwo** |

Produktem tego etapu analizy ryzyka jest lista ryzyk z przypisanymi poziomami wartości. Na jej podstawie organizacja powinna przygotować plan postępowania z ryzykiem obejmujący priorytety, zgodnie z którymi będą wdrażane poszczególne sposoby postępowania z ryzykiem, wskazywane osoby odpowiedzialne za ich realizację oraz ustalane harmonogramy.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ****Lista ryzyk**** | ****Priorytet**** | ****Status(wybór)**** | ****Wariant postępowania z ryzykiem**** | ****Planowane działanie minimalizujące ryzyko**** | ****Osoba/jednostka organizacyjna odpowiedzialna za realizację rekomendacji**** | ****Zakładanytermin realizacji rekomendacji**** | ****Uwagi**** |
|  |  | otwarte |  |  |  |  |  |
|  |  | otwarte |  |  |  |  |  |
|  |  | otwarte |  |  |  |  |  |
|  |  | otwarte |  |  |  |  |  |