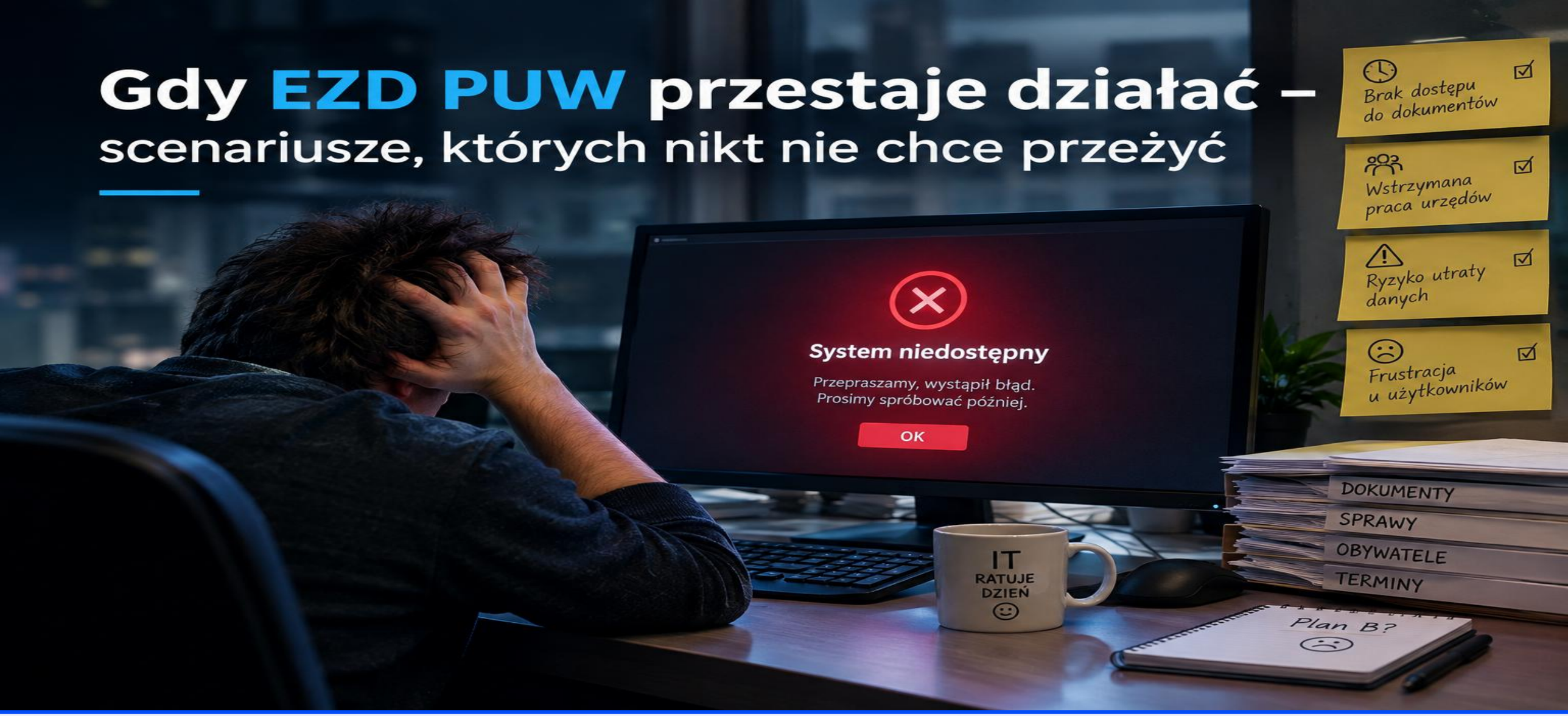
Gdy EZD PUW przestaje działać – scenariusze, których nikt nie chce przeżyć



w ramach zadania pn.: „Rozwój, wdrażanie i upowszechnianie systemu do elektronicznego zarządzania dokumentacją w podmiotach publicznych" [EZD-DOTACJA] finansowanego ze środków budżetu państwa w ramach dotacji celowej Ministra Cyfryzacji realizowanego przez NASK

NASK

PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTRA CYFRYZACJI

Jacek Nazaruk, Zespół Wsparcia Technicznego

08:07

Poniedziałek

Pierwsze zgłoszenie już jest.
Kto przejmuje koordynację działań?

**„Nie mogę wejść do EZD.
Pilne pismo czeka na wysyłkę.”**



Administrator weryfikuje i ustala priorytet

Czy problem występuje **tylko na jednym komputerze?**

Czy to wina **przeglądarki?**

Jaki jest **priorytet pisma?**

- Pilne
- Ważne
- Standardowe



1. Sprawdzenie stanowiska
2. Test przeglądarki
3. Ustalenie priorytetu pisma
4. Przekazanie dalszych działań

08:12 Problem rozwiązany!

- Sprawdzenie stanowiska
- Weryfikacja przeglądarki
- Ustalenie priorytetu pisma
- Zastosowanie rozwiązania



Analiza problemu → Weryfikacja przyczyny → Wdrożenie rozwiązania → Pismo pilne wysłane

SCENARIUSZ 1

Nikt nie może się zalogować



1 USTAL SKALĘ PROBLEMU

- Sprawdź, czy problem dotyczy jednego komputera, całego działu czy wielu pracowników w urzędzie.
- Porównaj zgłoszenia z różnych stanowisk i lokalizacji.
- Ustal, czy wszyscy widzą ten sam komunikat błędu.

2 USTAL, KIEDY PROBLEM SIĘ ROZPOCZĄŁ

- Kiedy ostatnio można było poprawnie zalogować się do EZD PUW?
- Czy przed awarią wykonywano aktualizacje, zmiany konfiguracji lub prace serwisowe?
- Zapisz godzinę pierwszego zgłoszenia i objawy problemu.

3 SPRAWDŹ PODSTAWOWE ELEMENTY

- **Sieć** – czy stanowiska mają dostęp do sieci i innych usług?
- **Adres aplikacji** – czy strona EZD PUW otwiera się na kilku komputerach?
- **Logowanie** – czy problem dotyczy **uwierzytelniania,** konkretnego użytkownika czy wszystkich kont?
- **Dostępność usługi** – sprawdź stan aplikacji i zależnych usług zgodnie z konfiguracją instalacji.

4 ZBIERZ DOWODY I KOORDYNUJ DZIAŁANIA

- Zapisz komunikaty błędów, czas wystąpienia i wyniki testów.
- Prowadź jeden rejestr wykonanych czynności oraz ich rezultatów.
- Przekaż koordynatorowi informację o skali problemu i wpływie na pracę urzędu.

MOŻLIWE PRZYCZYNY

(hipotezy, nie diagnoza)

- Niedostępność aplikacji / serwera EZD
- Problem sieciowy (lokalny lub w całej jednostce)
- Błąd mechanizmu uwierzytelniania (np. AD, SSO)
- Nieprawidłowa konfiguracja
- Przeciążenie usług
- Zmiany po aktualizacji

CZEGO NIE ROBIĆ?

- Nie diagnozuj na podstawie jednego zgłoszenia.
- Nie uruchamiaj jednocześnie wielu nieskoordynowanych prób naprawy.
- Nie restartuj masowo usług i serwerów.

NAJPIERW USTAL ZAKRES AWARII.

Następnie diagnozuj przyczynę.
Dopiero potem wdrażaj rozwiązanie.

Co zatrzymuje się razem z EZD

Rejestracja wpływów	›	Kancelaria gromadzi zaległości
Dostęp do akt	›	Pracownik nie otwiera dokumentów sprawy
Akceptacja dokumentów	›	Pisma czekają na decyzję lub podpis
Wysyłka korespondencji	›	Niepewność co do statusu pilnych pism



NASK

Pierwsze 15 minut

0–3

Zakres

- Kto nie pracuje?
- Od kiedy?
- Jakie czynności są problematyczne?

3–5

Prowadzenie

- Koordynator i wspólny kanał komunikacji
- Dziennik działań (zapisuj co, kto i kiedy)

5–10

Diagnoza

- Logi i zasoby
- Ostatnie zmiany i zadania okresowe
- Ochrona danych i integralność

10–15

Komunikat

- Stan awarii
- Proponowany tryb zastępczy
- Czas kolejnej aktualizacji

Komunikat podczas awarii

PRZYKŁAD KOMUNIKATU

„Od 08:07 system **EZD PUW jest niedostępny** dla pracowników jednostki. Trwa diagnostyka. Pilne sprawy zgłaszajcie koordynatorowi awarii. Obowiązuje zatwierdzona procedura zastępcza. Kolejną informację przekażemy o 08:30.”

Godzina rozpoczęcia	Status	Kolejna informacja
08:07	**Trwa diagnostyka**	**08:30**



Role podczas awarii

Rola	Główna odpowiedzialność
Koordynator	Prowadzi dziennik i komunikuje decyzje
Administrator IT	Diagnozuje oraz odtwarza usługę
Kancelaria	Ustala priorytet pism i rejestruje zaległości
Kierownictwo	Zatwierdza tryb pracy i priorytety

SCENARIUSZ 2

System działa zbyt wolno

CO WIDZI UŻYTKOWNIK?

- Długie wczytywanie ekranów i list dokumentów.
- Zapisywanie dokumentu trwa znacznie dłużej niż zwykle.
- Częste komunikaty „Ładowanie…” lub brak reakcji po kliknięciu.
- Operacje kończą się błędem lub nie pojawia się potwierdzenie.

NAJCZĘSTSZA REAKCJA

„ Klikam drugi raz, bo nic się nie dzieje.”

JAK POSTĘPOWAĆ?

1. Nie ponawiaj od razu tej samej operacji.
2. Poczekaj na wynik lub komunikat.
3. Sprawdź, czy dokument został zapisany (lista lub historia).
4. Jeśli problem trwa, zgłoś czas i objawy administratorowi.



Nie twórz duplikatów przez wielokrotne klikanie. System może nadal przetwarzać żądanie.

SCENARIUSZ 2

Diagnostyka administratora

Spowolnienie jest objawem, a nie diagnozą.



1 CZAS TYPOWYCH CZYNNOŚCI

- Porównaj czas otwierania dokumentu, zapisu i wyszukiwania z typowym działaniem.
- Sprawdź, czy problem dotyczy wielu użytkowników.
- Ustal, od kiedy występuje spowolnienie.

2 OBCIĄŻENIE SERWERA I DYSKÓW

- Sprawdź wykorzystanie CPU i pamięci RAM.
- Zweryfikuj obciążenie dysków, czas odczytu/zapisu i wolne miejsce.
- Sprawdź stan usług i logi błędów.

3 OCZEKIWANIE OPERACJI W BAZIE

- Sprawdź długie zapytania i blokady.
- Zweryfikuj aktywne sesje i czas wykonywania operacji.
- Porównaj wyniki z wcześniejszym okresem.

4 OSTATNIE ZMIANY I ZADANIA OKRESOWE

- Sprawdź aktualizacje lub zmiany konfiguracji.
- Zweryfikuj zadania cykliczne, raporty i indeksowanie.
- Ustal, czy problem ma charakter stały czy okresowy.

Nie uruchamiaj jednocześnie wielu nieskoordynowanych prób naprawy.

Najpierw zbierz dane i porównaj wyniki.
Dopiero potem wdrażaj rozwiązanie.

Sprawa jest. Załącznika brak

SCENARIUSZ 3

SYTUACJA

Widać metadane sprawy.
Otwarcie dokumentu kończy się błędem.

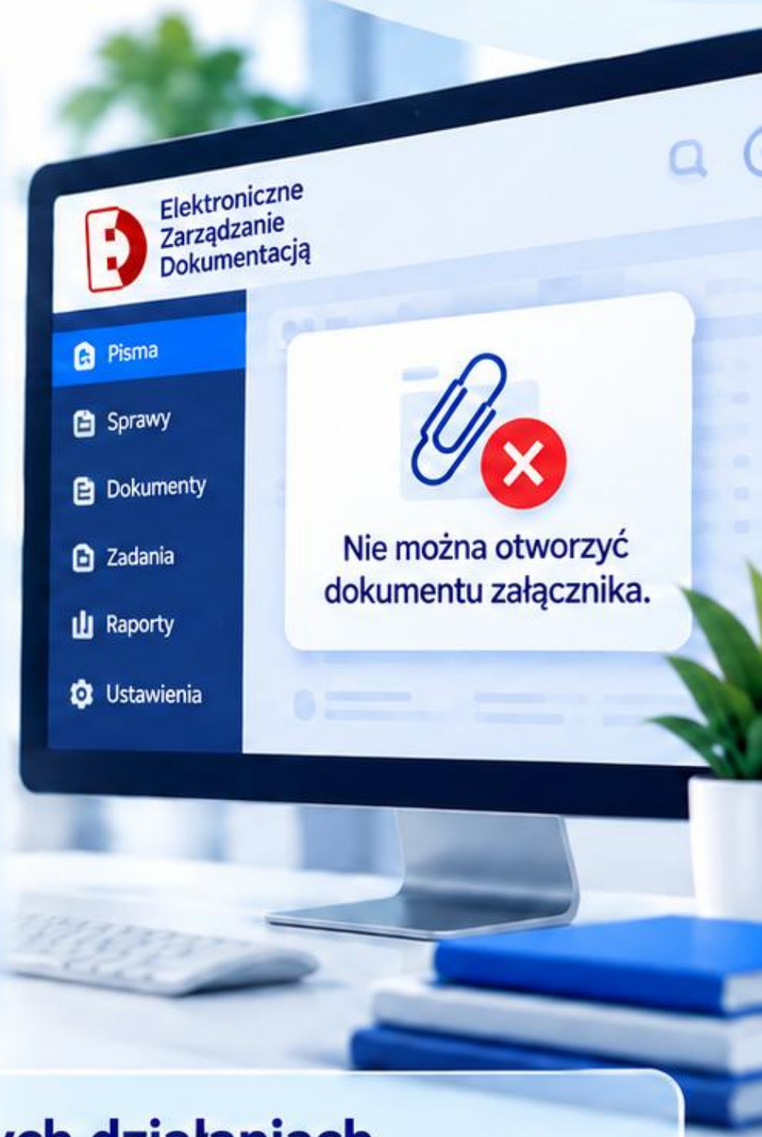
DO SPRAWDZENIA

1. **Uprawnienia do dokumentu**
   Sprawdź, czy masz wymagane uprawnienia do załącznika.

2. **Dostęp do miejsca zapisu plików**
   Upewnij się, że lokalizacja załączników jest dostępna (np. udział sieciowy). oraz masz do niej dostęp.

3. **Zakres i moment pojawienia się braków**
   Sprawdź, czy problem dotyczy jednego dokumentu, wielu spraw, a także od kiedy występuje.

4. **Prawidłowe działanie proxy oraz wersja Addina**
   Zweryfikuj, czy proxy działa poprawnie oraz czy zainstalowana wersja Addina jest zgodna z wersją EZD PUW.



Najpierw ustal zakres problemu, potem zdecyduj o dalszych działaniach.

SCENARIUSZ 4

Po aktualizacji pojawiają się błędy

01

Wstrzymanie kolejnych zmian

Zespół zapisuje wersje, zakres aktualizacji i logi błędów.

02

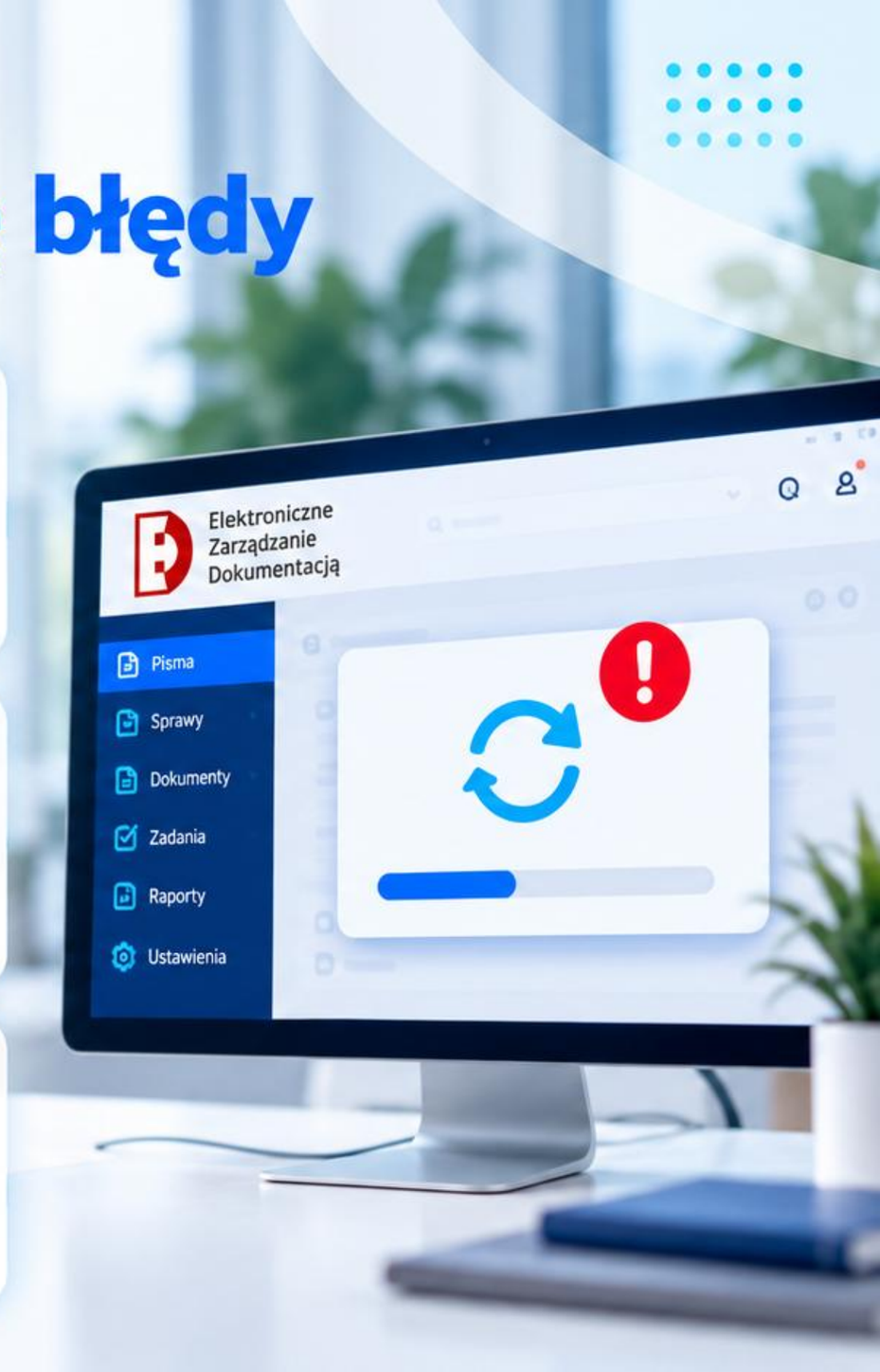
Zespół porównuje zachowanie

Testuje te same czynności w przygotowanym środowisku.

03

Wycofanie wymaga planu

Plan obejmuje aplikację, konfigurację i zgodność bazy.



SCENARIUSZ 5

Ransomware odcina dostęp do akt



IT izoluje zagrożone systemy i chroni kopie zapasowe.



Zespół bezpieczeństwa zabezpiecza ślady i prowadzi obsługę incydentu.



SCENARIUSZ 5

Ransomware odcina dostęp do akt

IT izoluje zagrożone systemy i chroni kopie zapasowe.

Zespół bezpieczeństwa zabezpiecza ślady i prowadzi obsługę incydentu.



01

Wykrycie i zgłoszenie incydentu

Niezwłocznie zgłoś podejrzenie ataku ransomware ustalonym kanałem. Zapisz godzinę wykrycia, objawy i zakres problemu.

02

Analiza i klasyfikacja

Zbierz dostępne logi, alerty i zgłoszenia.
Oceń wpływ incydentu na poufność, integralność i dostępność danych oraz usług EZD PUW.

03

Eskalacja i powołanie zespołu

Koordynator uruchamia właściwą ścieżkę eskalacji.
Do incydentu angażowany jest zespół odpowiedzialny za obsługę incydentów.

04

Powstrzymanie ataku

Izoluj zagrożone systemy i urządzenia. W razie potrzeby blokuj konta lub dostępy administracyjne, wstrzymaj zagrożone procesy i synchronizacje. Zabezpiecz logi oraz kopie zapasowe.

SCENARIUSZ 5

Ransomware – dalsze kroki i zamknięcie

Postępowanie zgodne z procedurą zarządzania incydentami dla EZD PUW.



WAŻNE

- Minimum **24 godziny** monitorowania po naprawie.
- **Do 2 dni roboczych** od zamknięcia — spotkanie podsumowujące i raport końcowy.
- **Do 24 godzin** — zgłoszenie do właściwych organów, jeśli incydent spełnia kryteria raportowania.

05 Eliminacja przyczyny

Ustal źródło incydentu i usuń przyczynę zagrożenia. Działania naprawcze koordynuj i dokumentuj.

06 Przywrócenie danych i usług

Odtwórz dane z właściwej, bezpiecznej kopii dopiero po opanowaniu zagrożenia. Sprawdź integralność danych oraz przeprowadź testy funkcjonalne i wydajnościowe.

07 Monitorowanie i zamknięcie

Monitoruj usługę minimum 24 godziny po naprawie i testach. Zamknij incydent dopiero po potwierdzeniu prawidłowego działania, wysłaniu komunikatu końcowego i uzupełnieniu rejestru.

08 Analiza po incydencie

Przygotuj raport końcowy, przeanalizuj przyczynę źródłową i określ działania zapobiegawcze.

Nie przywracaj kopii zapasowej, dopóki zagrożenie nie zostanie opanowane, dostęp atakującego ograniczony, a przyczyna usunięta.

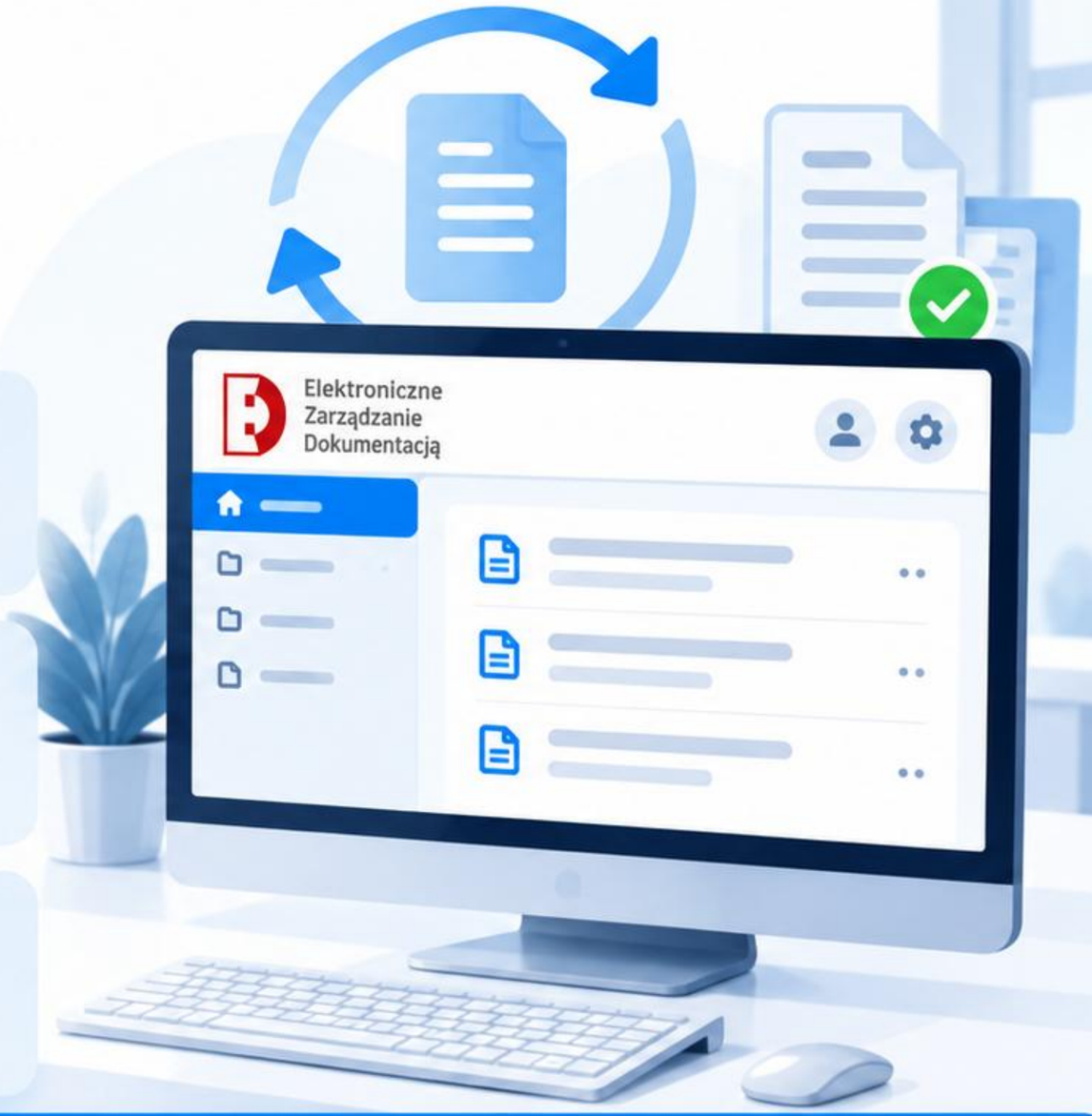
Odtworzenie, które przywraca pracę

TEST CAŁEJ USŁUGI

01 Logowanie właściwego użytkownika

02 Otwarcie historycznego załącznika

03 Kontrolowany zapis testowy



Kancelaria potwierdza możliwość pracy.

PROCEDURA KANCELARYJNA

Powrót do EZD PUW — bez duplikatów i luk

Przywrócenie dostępności to dopiero początek: trzeba jeszcze rozliczyć wszystkie czynności wykonane w trybie zastępczym.

01

Potwierdź dostępność

IT potwierdza przywrócenie systemu i stabilność podstawowych funkcji.

02

Porównaj rejestry

Zestaw rejestr zastępczy z dokumentami i statusami widocznymi w EZD PUW.

03

Uzupełnij braki

Wprowadź brakujące dokumenty i odwzorowania zgodnie z procedurą.

04

Sprawdź kompletność

Zweryfikuj załączniki, powiązania, terminy, nadania i historię czynności.

05

Zamknij tryb awaryjny

Odnotuj rozliczenie, wyjaśnij rozbieżności i poinformuj pracowników o powrocie.

Po odtworzeniu sprawdź: status dokumentu • kompletność załączników • powiązania ze sprawą • historię czynności

Kontroluj duplikaty przed rejestracją — nie zakładaj ponownie dokumentu tylko dlatego, że był obsługiwany w trybie zastępczym.

RTO i RPO: decyzje przed awarią

RTO — czas przywrócenia

Jak szybko chcemy przywrócić usługę?

4 h

Przykład: usługa ma wrócić do działania w ciągu 4 godzin.

RPO — punkt odtworzenia

Ile danych możemy maksymalnie utracić?

1 h

Przykład: odtworzone dane nie powinny być starsze niż 1 godzina.



Co trzeba ustalić przed awarią?

Priorytety procesów
Co musi wrócić jako pierwsze?

Backup i odtworzenie
Czy kopie pozwalają osiągnąć cele?

Test w praktyce
Zmierz rzeczywisty czas odtworzenia.

Odpowiedzialność
Kto zatwierdza cele i ogłasza powrót do pracy?

4 h i 1 h to wartości przykładowe — cele musi zatwierdzić i przetestować jednostka.

KRYTERIA ESKALACJI

Kiedy incydent wymaga eskalacji?

Incydent eskalacyjny to zdarzenie, które istotnie wpływa na dostępność, bezpieczeństwo lub integralność danych w usłudze EZD PUW.

Wymaga eskalacji

Zgłoś zdarzenie do **Zespołu Zarządzania Incydentami (IMT)** – uruchom procedurę zarządzania incydentami eskalacyjnymi.

Całkowita niedostępność usługi
Brak dostępu do EZD PUW lub brak możliwości korzystania z podstawowych funkcji.

Poważny incydent bezpieczeństwa
Zagrożenie poufności, integralności lub dostępności danych (np. nieautoryzowany dostęp, wyciek danych).

Atak ransomware
Szyfrowanie danych, żądanie okupu, złośliwe oprogramowanie zagrażające ciągłości działania.

Poważne zakłócenia działania
Długotrwałe błędy, awarie lub zdarzenia uniemożliwiające realizację kluczowych procesów w EZD PUW.

Nie wymaga eskalacji

Może być obsłużone w standardowym trybie działania (np. przez Zespół Wsparcia Użytkownika).

Krótkotrwałe spowolnienia
Czasowe pogorszenie wydajności usługi, bez całkowitej niedostępności.

Pojedyncze błędy funkcjonalne
Błędy dotyczące ograniczonego zakresu funkcji, z dostępnym obejściem.

Incydenty o niskim wpływie
Zdarzenia niepowodujące istotnego wpływu na dostępność, bezpieczeństwo ani integralność danych.

Pytania i zgłoszenia użytkowników
Problemy techniczne, które można rozwiązać w standardowym trybie wsparcia.

Zasada ostrożności

W przypadku wątpliwości, czy zdarzenie wymaga eskalacji, należy przyjąć wyższą kategorię klasyfikacji i zgłosić incydent do **Zespołu Zarządzania Incydentami (IMT)**.

Lepiej zgłosić incydent **niż pominąć istotne zagrożenie**.

PO ZAKOŃCZENIU AWARII

System wrócił. Czy możemy już pracować?

1

LOGOWANIE

Czy użytkownicy mogą wejść do systemu?

2

NAJWAŻNIEJSZE FUNKCJE

Czy działa rejestracja, dostęp do dokumentów i wysyłka?

3

DANE

Czy dokumenty i załączniki są kompletne?

4

STATUSY

Czy wiadomo, które operacje zakończyły się powodzeniem?

5

ZALEGŁOŚCI

Czy sprawy obsługiwane w trybie zastępczym zostaną uzupełnione?

6

DOKUMENTACJA

Czy zapisano przyczynę, działania i sposób zamknięcia awarii?

Powrót do pracy potwierdzamy testami i komunikatem — nie samym ekranem logowania.

KLASYFIKACJA

Nie każda awaria ma ten sam priorytet



PROBLEM LOKALNY

Jedno stanowisko

Sprawdź komputer, sieć, przeglądarkę i konto.



PROBLEM OGRANICZONY

Jedna funkcja lub grupa

Sprawdź zakres, dostępne obejście i wpływ na pracę.



PROBLEM KRYTYCZNY

Wielu użytkowników lub dane

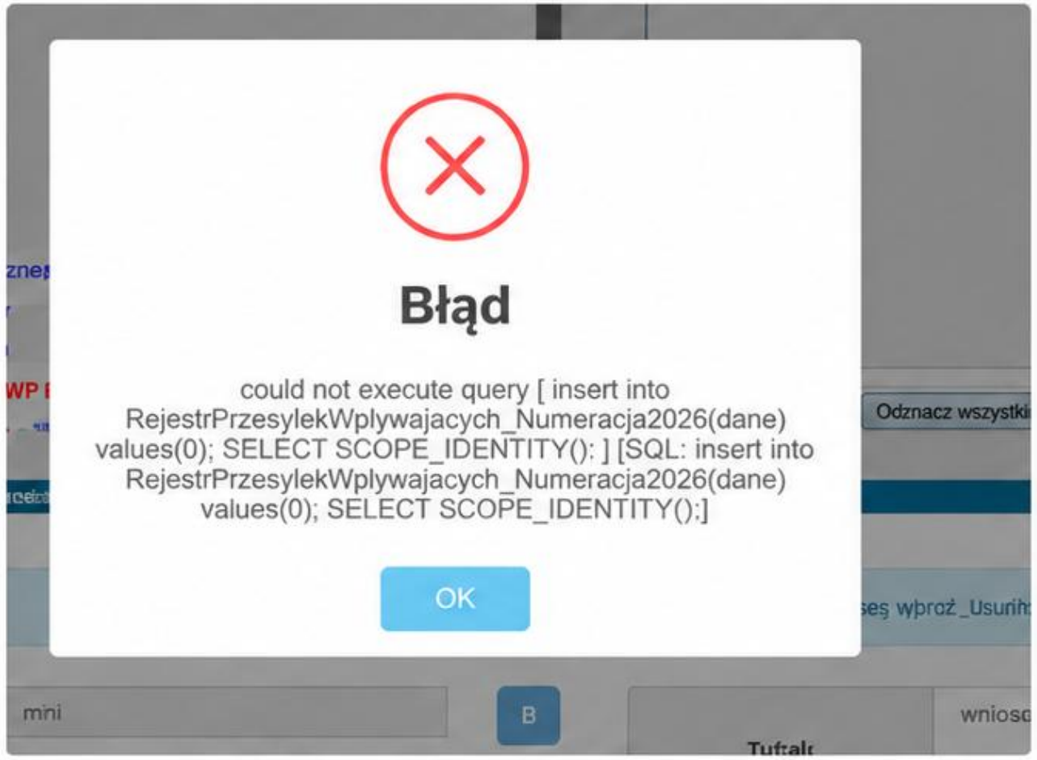
Pilna eskalacja zgodnie z procedurą i ochroną informacji.

SKUTEK DLA UŻYTKOWNIKÓW

Kancelaria nie może rejestrować wpływów

Próba rejestracji przesyłki kończy się błędem, ponieważ system odwołuje się do tabeli na 2026 rok.

Komunikat błędu podczas rejestracji przesyłki



Komunikat wskazuje próbę zapisu do tabeli Numeracja2026.

Skutek dla kancelarii

Nie można zarejestrować nowych przesyłek wpływających w 2026 roku. Operacja kończy się błędem.

Co należy zrobić?

1. Zweryfikować brak tabeli oraz historię wykonania skryptu tworzącego rejestr.
2. Wykonać zatwierdzony skrypt dla 2026 roku zgodnie z procedurą administracyjną.
3. Sprawdzić utworzenie rejestru i wykonać kontrolny test rejestracji wpływu.

PRZYCZYNA PROBLEMU

Brakuje rejestru RPW na 2026 rok

Na liście tabel w bazie danych są rejestry z lat 2019–2025, ale nie ma pozycji dla nowego roku.



LISTA TABEL W BAZIE DANYCH

- dbo.RejestrPrzesylekWplywajacych_Numeracja2019
- dbo.RejestrPrzesylekWplywajacych_Numeracja2020
- dbo.RejestrPrzesylekWplywajacych_Numeracja2021
- dbo.RejestrPrzesylekWplywajacych_Numeracja2022
- dbo.RejestrPrzesylekWplywajacych_Numeracja2023
- dbo.RejestrPrzesylekWplywajacych_Numeracja2024
- dbo.RejestrPrzesylekWplywajacych_Numeracja2025

W widocznym spisie ostatni rejestr numeracji dotyczy 2025 roku.

Dostępne lata

2019 2020 2021 2022 2023 2024 2025

26 RPW — Czego brakuje?

Tabeli rejestru przesyłek wpływających na rok 2026.

Oczekiwana nazwa tabeli

dbo.RejestrPrzesylekWplywajacych_Numeracja2026

Rejestr na 2026 rok nie występuje w widocznym spisie.

Wniosek: brak tabeli RPW 2026 w bazie danych

Koniec wsparcia oprogramowania w latach 2026–2027

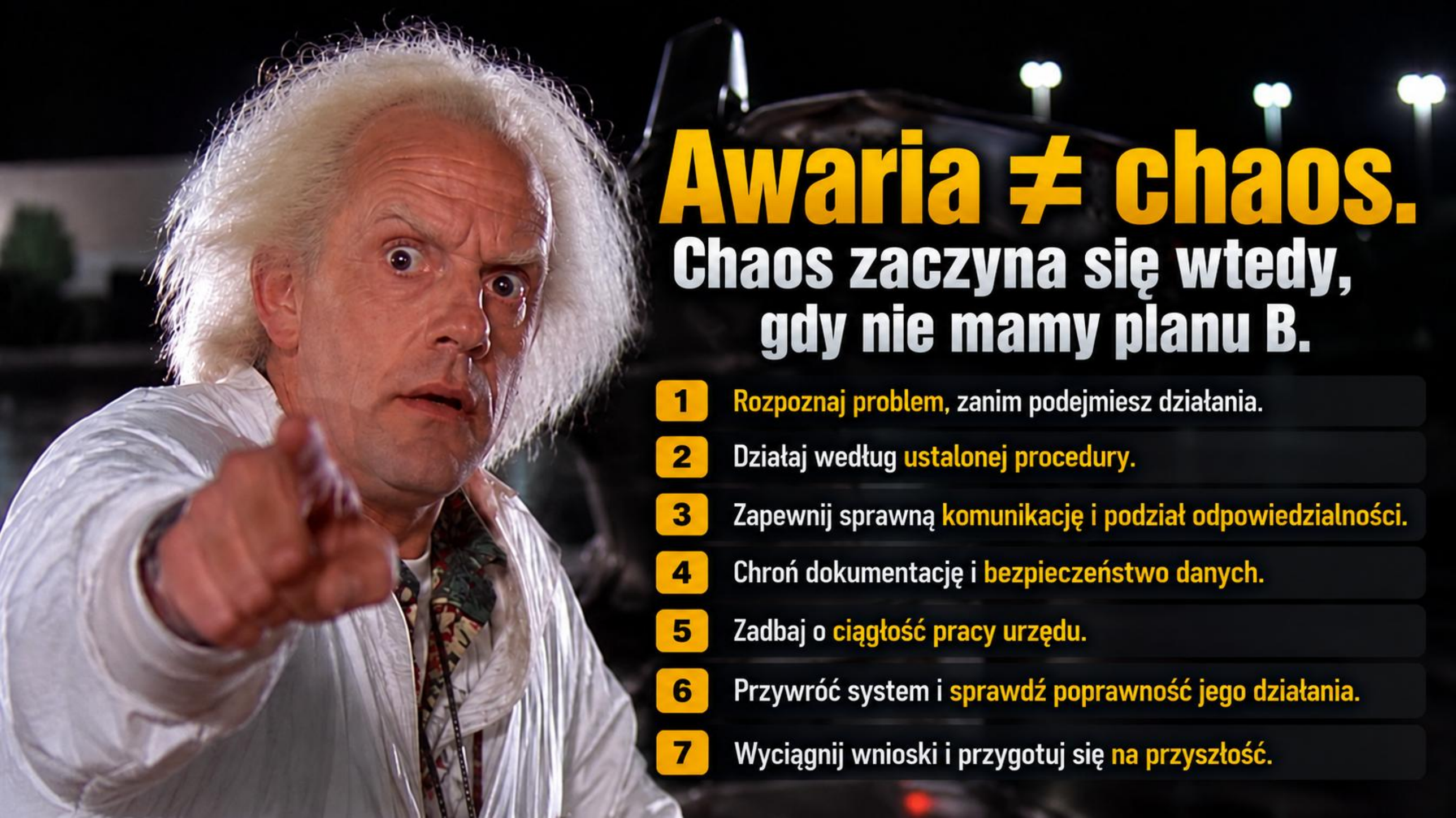
Sprawdź, które wersje i edycje tracą wsparcie oraz zaplanuj odpowiednie działania.

PRODUKT	KONIEC WSPARCIA	RODZAJ WSPARCIA	CO TO OZNACZA?
Office 2021 / Office LTSC 2021	13 października 2026	Rozszerzone	Koniec wsparcia i aktualizacji zabezpieczeń.
Windows 11 24H2 (Home/Pro)	13 października 2026	Podstawowe	Koniec obsługi tej wersji dla edycji Home i Pro.
Windows 10 22H2 (standardowe edycje)	14 października 2025	Podstawowe	Wsparcie zakończone (wyjątki: ESU i LTSC).
Windows Server 2016	12 stycznia 2027	Rozszerzone	Koniec wsparcia rozszerzonego.
Windows Server 2019	9 stycznia 2029	Rozszerzone	Koniec wsparcia rozszerzonego.
SQL Server 2019	8 stycznia 2030	Rozszerzone	Koniec wsparcia rozszerzonego.
SharePoint Server 2019	14 lipca 2026	Rozszerzone	Koniec wsparcia rozszerzonego.
.NET 6 LTS	12 listopada 2024	Standardowe	Wsparcie zakończone.
.NET 8 LTS	10 listopada 2026	Standardowe	Najbliższy termin do sprawdzenia.



Co powinien zrobić urząd?

1. **Zinwentaryzować używane wersje**
   Sprawdź, jakie wersje systemów, aplikacji i komponentów są używane w urzędzie.
2. **Sprawdzić daty końca wsparcia**
   Porównaj wersje z oficjalnym cyklem życia producenta.
3. **Zaplanować aktualizację lub migrację**
   Określ priorytety i zaplanuj działania z odpowiednim wyprzedzeniem.
4. **Zabezpieczyć budżet i zasoby**
   Uwzględnij koszty licencji, kompatybilność i czas wdrożenia.



Awaria ≠ chaos.

Chaos zaczyna się wtedy, gdy nie mamy planu B.

1. **Rozpoznaj problem,** zanim podejmiesz działania.
2. Działaj według **ustalonej procedury.**
3. Zapewnij sprawną **komunikację i podział odpowiedzialności.**
4. Chroń dokumentację i **bezpieczeństwo danych.**
5. Zadbaj o **ciągłość pracy urzędu.**
6. Przywróć system i **sprawdź poprawność jego działania.**
7. Wyciągnij wnioski i przygotuj się **na przyszłość.**

Elektroniczne Zarządzanie Dokumentacją

Jacek Nazaruk

Starszy specjalista ds. eAdministracji



NASK