
Bezpieczne prowadzenie obiektu wystawienniczego

Dlaczego muzeum, centrum nauki lub centrum doświadczeń marki należy prowadzić jak dobrze zarządzane środowisko IT i jak robi to taleor: każde urządzenie zidentyfikowane, każde połączenie szyfrowane, każda zmiana przypisana do osoby, każdy zwiedzający anonimowy.

Biała księga · październik 2026 · wersja 1.0

Dla dyrektorów, kierowników działów technicznych i IT, integratorów AV, konsultantów oraz komisji przetargowych muzeów, centrów nauki, centrów doświadczeń marki, obiektów dziedzictwa kulturowego i atrakcji turystycznych.

taleor

Spis treści

1	Streszczenie	3
2	Problem: obiekt to dziś infrastruktura IT	3
3	Czego naprawdę potrzebuje obiekt	5
4	Jak działa taleor	6
5	Bezpieczny od podstaw	8
6	Konfiguracja z pomocą asystenta	13
7	Analityka: czego dowiaduje się obiekt	14
8	Działa wszędzie, współpracuje z tym, co Państwo już mają	15
9	Modele wdrożenia i sposób oceny	17
10	O taleor	19
	Źródła i weryfikacja	19

1 Streszczenie

Obiekt wystawienniczy był kiedyś budynkiem, w którym stało kilka ekranów. Dziś jest siecią: to setki komputerów, wyświetlaczy, projektorów, głośników, opraw oświetleniowych i czujników od kilkunastu producentów, z których każde urządzenie ma własne oprogramowanie układowe, adres, a często także hasło. Obsługuje je niewielki zespół, który nie jest zespołem IT.

W niniejszym dokumencie wykazujemy, że obiektem należy zarządzać tak, jak zarządza się dobrze nadzorowaną infrastrukturą IT: każde urządzenie zidentyfikowane, każde połączenie szyfrowane, każda zmiana przypisana do osoby, każda aktualizacja zweryfikowana, każdy zwiedzający anonimowy. W rozdziale 3 przedstawiamy siedem zasad, rozdziały od 4 do 8 opisują, jak taleor je spełnia, a rozdział 9 zamyka lista kontrolna, którą komisja przetargowa może przedstawić każdemu dostawcy, także nam.

taleor to bezpieczny, agentowy sposób prowadzenia obiektu wystawienniczego: jego treści, aplikacji interaktywnych, odtwarzaczy i sprzętu z jednej konsoli. Opiera się na trzech filarach: jest bezpieczny od podstaw; konfiguruje go asystent, który nigdy nie wprowadza zmiany bez akceptacji imiennie wskazanej osoby; a jego analityka pokazuje „nie zmierzono” zamiast zera. Działa jako aplikacja webowa, jako aplikacja desktopowa dla systemów Windows, macOS i Linux oraz jako serwer lokalny w Państwie własnym budynku, także w trybie całkowicie izolowanym, bez dostępu do internetu. Jego odtwarzacze działają na systemach Windows, macOS, Linux, Raspberry Pi i Android. Steruje sprzętem dowolnej marki za pomocą otwartych standardów.

2 Problem: obiekt to dziś infrastruktura IT

2.1 Setki urządzeń, dziesiątki marek, niewielki zespół

Wystarczy policzyć komputery na ekspozycji współczesnego muzeum: po jednym za większością eksponatów, do tego sieciowe wyświetlacze, projektory, procesory audio, kontrolery oświetlenia, czujniki, czytniki i przyciski. W obiekcie średniej wielkości ich liczba sięga kilkuset. Przykładowe dane użyte do opracowania taleor, wzorowane na typowym muzeum regionalnym, obejmują 69 eksponatów i 342 urządzenia, które posługują się 49 protokołami sterowania. To zwyczajna infrastruktura.

Każdy producent wnosi własny protokół, własne narzędzie do zarządzania i własne wyobrażenie o tym, jak powinny działać aktualizacje. Treści zmieniają się co sezon. Zespół liczy zwykle od dwóch do pięciu osób, których zakres

obowiązków nie przewidywał zarządzania flotą urządzeń ani instalowania poprawek.

2.2 Narażenie na zagrożenia

Cztery słabe punkty wzajemnie się wzmacniają.

Domyślne dane logowania. Profesjonalny sprzęt AV trafia do obiektu z interfejsem zarządzania i fabrycznym hasłem, które rzadko się zmienia, ponieważ zmiana na dwustu urządzeniach to tydzień pracy, za którą nikt nie odpowiada. Botnet Mirai z 2016 roku przejmował urządzenia, próbując krótkiej listy haseł fabrycznych. Sprzęt AV w obiektach wystawienniczych nie jest od tego wolny.

Niezaktualizowane odtwarzacze. Komputer za eksponatem często działa na tym samym systemie operacyjnym, z którym został oddany do użytku, ponieważ aktualizacja oznacza zamknięcie eksponatu. Niezaktualizowany komputer w tej samej sieci co system biletowy i system zarządzania budynkiem to otwarta droga do środka. Ramy, według których oceniane są instytucje publiczne w Niemczech, Holandii i Polsce (BSI IT-Grundschutz, Baseline Informatiebeveiliging Overheid oraz obowiązki wynikające z NIS2), traktują terminowe instalowanie poprawek i inwentaryzację zasobów jako podstawowe zabezpieczenia.

Wspólne sekrety. Wiele systemów sterowania uwierzytelnia odtwarzacz kluczem zapisanym w pliku konfiguracyjnym. Każdy, kto może odczytać ten plik, może podszyć się pod odtwarzacz.

Zależność od chmury. System, który przestaje działać, gdy zawodzi internet lub chmura dostawcy, przenosi pojedynczy punkt awarii tam, gdzie obiekt nie może go naprawić. Dla instytucji publicznej to także kwestia zamówień: kto przechowuje dane, na podstawie jakiego prawa i co się dzieje po wygaśnięciu umowy.

2.3 Przestoje, martwe pola i uzależnienie od dostawcy

Przestój to awaria najbardziej widoczna i najrzadziej mierzona. Ekran zawiesza się o dziesiątej, zwiedzający wspomina o tym w południe, technik dowiaduje się o czternastej, a cztery stracone godziny nigdzie nie zostają odnotowane.

Większość obiektów liczy zwiedzających przy wejściu i nigdzie indziej. Nie wiedzą, przy którym eksponacie ludzie się zatrzymali, na jak długo ani czy film obejrzano do końca. Tam, gdzie pomiar istnieje, jest to często osobny system, zbyt często oparty na kamerach, które identyfikują osoby.

Każdy podsystem przychodzi z własnym dostawcą i własną umową. Gdy dostawca zostaje przejęty lub wycofuje produkt, treści przygotowanych dla zamkniętego, firmowego odtwarzacza nie da się przenieść, a sprzęt, który komunikuje się tylko z jednym kontrolerem, staje się złomem. Komisja powinna pytać nie „czy ten dostawca obsługuje nasz sprzęt?”, lecz „gdyby ten dostawca zniknął, co nadal pozostałoby nasze?”

3 Czego naprawdę potrzebuje obiekt

Te problemy zostały już rozwiązane w ogólnym IT. Brakowało zastosowania tych rozwiązań do specyfiki obiektu wystawienniczego: wielu małych komputerów, wielu marek, niewielkiego zespołu, publiczności i budynku, który musi zostać otwarty o dziesiątej. Proponujemy siedem zasad.

1. **Każde urządzenie ma tożsamość, której nie da się skopiować.** Klucz wygenerowany na jego własnym sprzęcie, który nigdy go nie opuścił. Nie hasło. Nie token w pliku.
2. **Każde połączenie jest szyfrowane i uwierzytelniane w obu kierunkach.** Każde słabsze rozwiązanie pozwala obcej osobie w sieci obiektu podstawić wiarygodną podróbkę.
3. **Na odtwarzaczu nie uruchamia się nic, co nie zostało wcześniej zweryfikowane.** Sterowniki i aktualizacje są sprawdzane na odtwarzaczu na podstawie podpisu lub sumy kontrolnej, a nie tylko u źródła.
4. **Każda zmiana ma autora i czas.** Ślad audytowy, który administrator może skrócić do jednego dnia lub edytować, nie jest śladem audytowym.
5. **Ludzie otrzymują uprawnienia, których wymaga ich praca, i nic ponad to.** Kierownik techniczny może zrestartować zawieszony ekran, nie mając możliwości jego usunięcia.
6. **Zwiedzający pozostają anonimowi dzięki konstrukcji systemu, a nie na mocy regulaminu.** To właściwość schematu bazy danych, w dodatku sprawdzana testami.
7. **Obiekt jest właścicielem swojego systemu.** Może uruchomić wszystko we własnym budynku, bez internetu, i może zmienić dostawcę bez utraty treści.

Tego właśnie kompetentny dział IT wymagałby od każdej floty dwustu komputerów. Dalsza część dokumentu opisuje, jak taleor spełnia te zasady.

4 Jak działa taleor

4.1 Elementy systemu

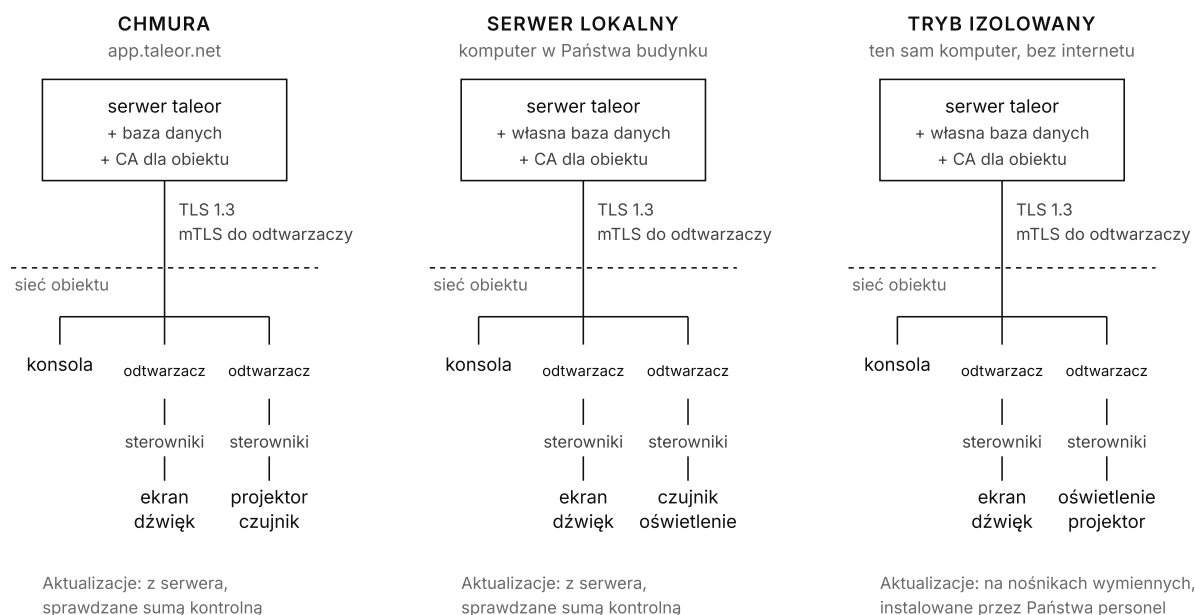
Konsola. Aplikacja webowa, w której personel widzi każdy eksponat, odtwarzacz i element sprzętu, wgrywa treści, ustawia harmonogramy i wyzwacze, śledzi stan techniczny i alerty oraz przegląda analitykę. Działa w każdej aktualnej przeglądarce lub jako aplikacja desktopowa dla systemów Windows, macOS i Linux.

Agent odtwarzacza. Niewielka usługa działająca w tle na komputerze za każdym eksponatem. Utrzymuje stałe, wzajemnie uwierzytelnione połączenie z serwerem, odtwarza to, co mu zlecono, steruje sprzętem obsługiwanym przez ten komputer, odczytuje jego czujniki, raportuje swój stan i sam się aktualizuje. Domyślnie przechowuje lokalną kopię swoich treści o rozmiarze 4 GB i nadal odtwarza, gdy serwer jest nieosiągalny. Agenci działają na systemach Windows, macOS, Linux, Raspberry Pi i Android. Ekran bez komputera paruje się jako odtwarzacz przeglądarkowy za pomocą sześciocyfrowego kodu odczytanego z ekranu.

Sterowniki. Podpisany pakiet, który informuje taleor, co potrafi dany element sprzętu i jak się z nim komunikować. Konsola zleca czynność, taką jak zasilanie, źródło czy głośność; sterownik przekłada ją na protokół.

Serwer. Baza danych, huby WebSocket przekazujące bieżący stan, urząd certyfikacji (CA) dla każdego obiektu, magazyn mediów, silnik harmonogramów, monitor alertów, dziennik audytu i analityka. To samo oprogramowanie działa w naszej chmurze lub na komputerze w Państwa budynku, z internetem lub bez niego.

4.2 Jedna wersja, trzy sposoby uruchomienia



Rysunek 1. Jedna wersja, trzy sposoby uruchomienia. Ten sam serwer, konsola i agenci odtwarzaczy w chmurze, na serwerze lokalnym w budynku lub w trybie izolowanym, bez internetu.

W trybie chmurowym konsola i serwer znajdują się pod adresem app.taleor.net, a agenci nawiązują z nimi połączenia wychodzące; sprzętem w sieci obiektu sterują agenci działający wewnątrz tej sieci. W trybie serwera lokalnego ten sam pakiet instaluje się na komputerze z systemem Windows, macOS lub Linux w budynku, z własną prywatną bazą danych i własnym urzędem certyfikacji, dzięki czemu konsola, odtwarzacze, media i dziennik audytu pozostają wewnątrz. W trybie izolowanym ten serwer działa całkowicie bez internetu: środowisko uruchomieniowe i baza danych są częścią pakietu, podczas instalacji nic nie jest pobierane, a aktualizacje dostarcza na nośnikach wymiennych Państwa własny personel. Jedna baza kodu, jedna konsola; obiekt, który zaczyna w chmurze, może później przenieść system do siebie.

5 Bezpieczny od podstaw

5.1 Tożsamość: klucz, który nigdy nie opuszcza komputera

talear zastępuje wspólny sekret certyfikatem. Podczas rejestracji odtwarzacz generuje na własnym komputerze asymetryczną parę kluczy i wysyła wyłącznie jej część publiczną, w żądaniu podpisania certyfikatu, do urzędu certyfikacji obiektu, który podpisuje i odsyła certyfikat. Klucz prywatny nigdy nie jest przesyłany. Od tej chwili odtwarzacz potwierdza swoją tożsamość, składając podpis na bieżąco podczas każdego uzgadniania połączenia TLS. Nie ma niczego, co można by skopiować.

Jeden urząd certyfikacji na obiekt, uruchamiany z konsoli przez administratora. Przejęcie kontroli w jednym obiekcie nie pozwala wygenerować tożsamości w innym. Klucz prywatny urzędu jest przechowywany w postaci zaszyfrowanej przy użyciu sekretu odrębnego od pozostałych sekretów serwera.

Żądanie nie jest traktowane jako zaufane. Z żądania podpisania pobierany jest wyłącznie klucz publiczny; podmiot, okres ważności i wszystkie rozszerzenia ustala serwer, więc odtwarzacz nie może poprosić o nazwę innego odtwarzacza ani o status urzędu certyfikacji. Certyfikaty odtwarzaczy są wystawiane wyłącznie do uwierzytelniania klienta, więc za pomocą skradzionego certyfikatu nie da się uruchomić fałszywego serwera.

Nie ma przycisku „Wystaw certyfikat”. Certyfikat, którego klucz prywatny serwer kiedykolwiek posiadał, przekreślałby sens całego rozwiązania.

5.2 Transmisja: szyfrowana i sprawdzana w obu kierunkach

Każde połączenie między przeglądarką, odtwarzaczem i konsolą odbywa się przez TLS 1.3 (dla starszych klientów akceptowana jest wersja 1.2). Połączenia odtwarzaczy korzystają z wzajemnego TLS (mutual TLS): każda strona przedstawia drugiej swój certyfikat.

Ważny certyfikat jest warunkiem koniecznym, ale niewystarczającym. Przy każdym połączeniu serwer sprawdza dodatkowo, w bazie danych, a nie na liście z pamięci podręcznej, czy certyfikat nie został unieważniony ani nie wygasł, czy wskazane w nim urządzenie nadal istnieje i czy należy ono do obiektu, dla którego certyfikat wystawiono.

Certyfikaty są ważne 398 dni, co odpowiada górnemu limitowi CA/Browser Forum dla certyfikatów publicznie zaufanych, i odnawiają się w ostatnich 30 dniach ważności przez własne połączenie odtwarzacza z wzajemnym TLS, więc

flota wymienia poświadczenia bez wizyty na miejscu. Wystawienie nowego certyfikatu unieważnia poprzedni.

Włączanie wzajemnego TLS odbywa się etapami: tryb rotacji akceptuje zarówno certyfikat, jak i starsze poświadczenie, podczas gdy flota przechodzi na nowe rozwiązanie galeria po galerii, a tryb wymagany włącza się dopiero wtedy, gdy wszystkie punkty końcowe mają certyfikaty. Serwer odmawia tego przełączenia, dopóki którekolwiek z łączących się urządzeń zostałoby odcięte, ponieważ alternatywą jest ciemne muzeum. Przywrócenie trybu wyłączzonego natychmiast cofa zmianę.

5.3 Integralność: nie uruchamia się nic, co nie zostało zweryfikowane

Sterowniki są podpisane. Sterownik to pakiet z manifestem i odłączonym podpisem Ed25519 obejmującym skrót pakietu. Serwer produkcyjny domyślnie odrzuca niepodpisany pakiet, ponieważ sterownik to kod, który otwiera gniazda sieciowe i komunikuje się ze sprzętem. Integratorzy i producenci mogą tworzyć i podpisywać własne sterowniki za pomocą zestawu do tworzenia sterowników.

Suma kontrolna aktualizacji odtwarzacza jest weryfikowana. Serwer publikuje wersję wraz z jej sumą kontrolną SHA-256. Odtwarzacz przede wszystkim weryfikuje sumę kontrolną, następnie rozpakowuje aktualizację do katalogu przejściowego, podmienia wersję i uruchamia się ponownie. Nieudana weryfikacja oznacza odrzuconą aktualizację.

Aktualizacje uwzględniają pracę obiektu. Aktualizacja instaluje się wyłącznie poza godzinami otwarcia. Nowa wersja, która w ciągu dziesięciu minut nie przejdzie kontroli stanu, jest wycofywana i blokowana przed ponowną próbą. Obiekt może wyłączyć aktualizacje dla wybranego odtwarzacza; taki odtwarzacz, podobnie jak odtwarzacz pozostający w tyle, jest oznaczany w konsoli jako „nieaktualny”, dzięki czemu nigdy nie zostaje po cichu zapomniany.

5.4 Dostęp i role

taleor ma pięć ról, które można przypisywać.

Rola	Do czego służy
Administrator sieci	Wszystko, we wszystkich obiektach prowadzonych przez instytucję
Administrator organizacji	Wszystkie uprawnienia na poziomie obiektu, we wszystkich obiektach organizacji
Administrator obiektu	Wszystkie uprawnienia na poziomie obiektu, w jednym obiekcie
Menedżer treści	Treści, Reele, harmonogramy i szablony
Kierownik techniczny	Obsługa sprzętu: restart, zasilanie, źródło, głośność

Role są celowo ogólne, ponieważ modelu uprawnień, którego nikt nie potrafi wyjaśnić, nikt też nie stosuje. Każdy punkt końcowy API sprawdza zarówno rolę, jak i obiekt, więc osoba z uprawnieniami w jednym obiekcie nie widzi niczego z innego. Logowanie odbywa się indywidualnie, nigdy na wspólne konto; przy pierwszym użyciu nowego konta należy zmienić hasło.

5.5 Ślad audytowy

Każda operacja zapisu trafia do dziennika audytu wraz z osobą, czynnością, czasem i adresem sieciowym, z którego pochodziła. Dotyczy to również działań asystenta, które są rejestrowane jako zastosowane przez asystenta w imieniu wskazanej osoby. Dziennik można filtrować w konsoli i eksportować do pliku CSV z tymi samymi filtrami, dzięki czemu audytor może zabrać go ze sobą.

Dwie właściwości chronią dziennik przed osobami, które mają nad nim największą władzę. Dla klasy danych audytu obowiązuje wymuszony minimalny okres przechowywania wynoszący 180 dni: obiekt może przechowywać dziennik dłużej, nigdy krócej. Gdy zaś pracownik korzysta z prawa do usunięcia danych, jego konto zamienia się w znacznik usunięcia: dane identyfikacyjne zostają utajnione, adresy sieciowe usunięte, a czynności zachowane, więc dziennik nadal pokazuje, że ktoś, czyje dane później usunięto, opublikował scenę trzeciego dnia miesiąca. Administrator nie może usunąć własnego konta.

5.6 Prywatność zwiedzających wynikająca z konstrukcji

Zwiedzający obiekt to osoby z ogółu publiczności, w tym wiele dzieci. Właściwy projekt to taki, w którym system nie jest w stanie zarejestrować, kim są.

Dwie tabele przechowujące dane o zachowaniu zwiedzających, zdarzenia obecności i zdarzenia interakcji, zawierają obiekt, urządzenie, strefę, słowo opisujące stan lub zdarzenie oraz znacznik czasu. Nie zawierają żadnego identyfikatora osoby: żadnego adresu sieciowego, wizerunku twarzy, pliku cookie

ani sesji. To właściwość schematu, a nie obietnica zapisana w polityce; test sprawdza to na rzeczywistych definicjach tabel i przerywa kompilację, jeśli ktoś doda taką kolumnę.

Za tym stoi rejestr czynności przetwarzania, który istnieje w kodzie i jest weryfikowany w ramach tej samej zmiany co kod tworzący dane: cel, podstawa prawna, stopień identyfikacji, odbiorcy i okres przechowywania dla każdej klasy danych. Nocne zadanie porządkowe usuwa wiersze po upływie okresu przechowywania, partiami, aby nigdy nie spowalniać otwartego obiektu, i zapisuje wiersz z każdego przebiegu, także nieudanego. Ten zapis jest pierwszym dowodem, o który prosi audytor.

Klasa danych	Domyślny okres przechowywania	Minimum
Obecność przy ekspozycji	400 dni	1 dzień
Dotknięcia i wybory	400 dni	1 dzień
Co i kiedy odtworzono	1825 dni	365 dni
Logi odtwarzaczy	30 dni	1 dzień
Kto co zrobił (audyt)	730 dni	180 dni

Zabezpieczenia zbudowano zgodnie z wymaganiami technicznymi normy ISO/IEC 27701, rozszerzenia normy ISO/IEC 27001 dotyczącego prywatności. Do tego twierdzenia podchodzimy ostrożnie: produkt nie może uzyskać certyfikacji na zgodność z normą 27701; może ją uzyskać instytucja, po audycie. taleor wdraża zabezpieczenia, które norma ujmuje jako techniczne, i dostarcza dowodów potrzebnych audytorowi; instytucja nadal musi wyznaczyć osobę odpowiedzialną za ochronę prywatności, przeprowadzić ocenę skutków, zawrzeć umowy z podmiotami przetwarzającymi i umieścić informacje w galeriach.

5.7 Alarm

Jeden element sterujący uruchamia alarm w całym obiekcie, na jednym piętrze, w jednej strefie lub na wybranych odtwarzaczach. Komunikat zajmuje cały ekran, na dole ekranu przesuwają się powiadomienia, a dźwięk eksponatów cichnie. Odtwarzacz, który połączy się ponownie w trakcie komunikatu, również go otrzyma. Alarm można rozpocząć i zakończyć z pilota ręcznego personelu i jest on rejestrowany w dzienniku audytu jak każde inne działanie. Celowo mówimy „dźwięk eksponatów”: taleor wycisza to, czym steruje, i nie jest systemem nagłośnienia ogólnego.

5.8 Izolacja i tryb izolowany

Pakiet serwera lokalnego instaluje własny, prywatny klaster PostgreSQL, nasłuchujący wyłącznie na interfejsie pętli zwrotnej (loopback) i na niestandardowym porcie, dzięki czemu nigdy nie koliduje z bazą danych, która już istnieje na komputerze. Nikt nie wpisuje hasła do bazy danych: losowe hasło jest generowane podczas instalacji i przechowywane wyłącznie w pliku konfiguracyjnym, który mogą odczytać tylko system i jego administratorzy. Środowisko kontenerowe nie jest wymagane. Tryb izolowany to ten sam pakiet bez dostępu do internetu (punkt 4.2).

Sprzęt w sieci obiektu jest zawsze sterowany z wnętrza tej sieci, przez agentów odtwarzaczy lub serwer lokalny. Konsola w chmurze nigdy nie potrzebuje drogi do Państwa budynku; to agenci nawiązują połączenia wychodzące.

5.9 Bezpieczne zachowanie w razie awarii

- Odtwarzacz, który traci połączenie z serwerem, nadal odtwarza ostatnią poprawną konfigurację z lokalnej pamięci podręcznej, także po ponownym uruchomieniu, aż do powrotu serwera.
- Odtwarzacz, który przestaje odpowiadać, generuje alert z jego nazwą, lokalizacją, informacją, co powinien wyświetlać, i od kiedy. Alert znika samoczynnie, gdy odtwarzacz wraca; powtarzająca się usterka aktualizuje istniejący alert.
- Serwer wykonuje kopie zapasowe bazy danych zgodnie z harmonogramem, z krocącą historią i możliwością przywrócenia z dowolnego punktu. Wszystko, co usunięto z biblioteki treści, można odzyskać przez 30 dni.
- Serwer odmawia przełączenia obiektu w tryb wymaganego wzajemnego TLS, dopóki którekolwiek urządzenie zostałoby odcięte, odrzuca nieaktualny plan asystenta i odrzuca niepodpisany sterownik. Mając wybór między zgadywaniem a zatrzymaniem się, taleor zatrzymuje się i podaje powód.

5.10 Jak sprawdzamy własną pracę

Przed premierą konsola, odtwarzacz i witryna internetowa taleor przeszły przegląd bezpieczeństwa aplikacji: spisany model zagrożeń, exploity typu proof of concept dla każdej podejrzewanej słabości, skanery zależności i analizy statycznej oraz ponowne skanowanie po wprowadzeniu poprawek. Każde ustalenie ma przypisaną wagę, właściciela i zweryfikowaną poprawkę; etap kontrolny nie zostaje zaliczony, dopóki otwarte jest ustalenie blokujące. Tego samego warto wymagać od każdego dostawcy.

6 Konfiguracja z pomocą asystenta

6.1 Co robi asystent

Konfiguracja interaktywnego eksponatu zawsze była pracą specjalistyczną, którą w obiekcie potrafi wykonać jedna osoba. taleor ma w konsoli asystenta o nazwie Oli. Wystarczy wpisać, czego się oczekuje:

Gdy ktoś znajdzie się w odległości do metra od ekranu w holu, włącz film powitalny, a gdy przez trzydzieści sekund nikogo nie będzie, wróć do poprzedniej treści.

Asystent odczytuje konfigurację obiektu (eksponaty, odtwarzacze, Reele, zadeklarowane wejścia) i proponuje plan z dokładną listą zmian:

Odczyt: ekran w holu, zadeklarowany czujnik obecności, 2 Reele.
Propozycja: przy odległości 100 cm lub mniejszej odtwórz „film powitalny”, powrót po 30 s.
Czeka na Państwa akceptację.

Państwo czytają plan. Następnie wybierają Państwo „Zastosuj” lub „Odrzuć”. Gdy czegoś brakuje, asystent mówi czego: nie ma Reela o nazwie „film powitalny” albo przy tym odtwarzaczu nie ma czujnika obecności. Gdy prośba jest niejednoznaczna, zadaje po jednym pytaniu naraz i nigdy nie zakłada istnienia sprzętu, którego nie ma.

Asystent proponuje wyzwalacze, przypisania Reeli oraz włączenie wyzwalacza i stosuje je po Państwa akceptacji. Każdą funkcję nadal można obsługiwać ręcznie.

6.2 Model uprawnień

Asystent nie jest użytkownikiem uprzywilejowanym. Nie ma żadnych własnych uprawnień.

- **Odczyt.** Jego narzędzia do przeglądania obiektu działają tylko w trybie odczytu i są ograniczone do obiektu, w którym pracuje dana osoba.
- **Proponowanie.** Jego narzędzia do tworzenia planu jedynie zapisują proponowany krok. Nic nie zostaje wykonane. Jest to sprawdzane testami.
- **Zastosowanie.** Po wybraniu „Zastosuj” zapisane kroki przechodzą przez te same funkcje usług, walidację i kontrole uprawnień, jak gdyby dana osoba wprowadzała każdą zmianę ręcznie, więc osoba, która nie może czegoś

zmienić, nie może też zlecić tej zmiany asystentowi. Dziennik audytu zapisuje wynik jako zastosowany przez asystenta w imieniu wskazanej osoby.

- **Nieaktualność.** Plan, który stracił aktualność, bo między propozycją a akceptacją usunięto Reel, zostaje odrzucony, a nie uzupełniony domysłami.
- **Ograniczenie.** Gdy asystent nie jest skonfigurowany, jest wyłączony i ukryty. Jego użycie jest opomiarowane, ze sztywnym miesięcznym limitem dla całego serwera. Błędy usługi bazowej nigdy nie są wyświetlane dosłownie.

6.3 Dlaczego przegląd przed zastosowaniem

System, który zmienia to, co jest odtwarzane na dwustu ekranach, musi umieć odpowiedzieć na pytanie: „kto to zmienił i czy zatwierdził to człowiek?” Warto zadać to pytanie każdemu produktowi, który reklamuje automatyczną konfigurację.

7 Analityka: czego dowiaduje się obiekt

7.1 Na podstawie tego, co faktycznie raportują odtwarzacze

Analityka taleor, w konsoli nazywana „Statystyki”, powstaje na podstawie danych raportowanych przez odtwarzacze i czujniki, a nie przez osobny system liczący: czujnik, który uruchamia film, jest tym samym czujnikiem, który liczy, kto się zatrzymał i na jak długo. Każdą wartość można zawęzić do całego obiektu, piętra, strefy lub odtwarzacza, za dzisiaj, ten tydzień, ten miesiąc lub ten rok, z poprzednim okresem do porównania.

7.2 Co Państwo widzą

Natężenie ruchu i czas przebywania. Liczba zwiedzających na godzinę, dzień lub miesiąc, na podstawie czujników i dotknięć. Średni czas przebywania podczas zaangażowanych wizyt. Najbardziej obciążone strefy i godziny w postaci mapy cieplej stref w rozbiciu na godziny.

Co sprawdziło się najlepiej. Ranking eksponatów według liczby wizyt i czasu przebywania, dzięki któremu mało odwiedzany zakątek zostaje zauważony, zanim kurator go minie. Zwiedzający i czas przebywania są przypisani do eksponatu; czas pracy i odtworzenia do każdego odtwarzacza.

Dowód odtworzenia. Każda pozycja, każde odtworzenie, do końca lub nie, z eksportem do CSV uwzględniającym ten sam zakres i okres. Domyślnie przechowywane przez pięć lat, a więc dłużej niż trwa okres licencji czy umowa sponsorska.

Stan i czas pracy odtwarzaczy. Czas pracy każdego odtwarzacza w wybranym okresie, na podstawie migawek stanu. Brak migawek w danym okresie oznacza stan nieznan, a nie sprawny.

7.3 Uczciwe liczby

Wartość, której nie da się zmierzyć, jest opisana jako „nie zmierzono”, nigdy jako zero. Strefa bez czujnika nie raportuje zera zwiedzających; raportuje, że liczby zwiedzających w niej nie zmierzono.

7.4 Ponownie: prywatność wynikająca z konstrukcji

Zdarzenia, na których opiera się każda wartość, to zdarzenia opisane w punkcie 5.6, bez żadnego identyfikatora zwiedzającego: bez kamer, bez wykrywania twarzy, bez śledzenia urządzeń, bez plików cookie.

8 Działa wszędzie, współpracuje z tym, co Państwo już mają

8.1 Platformy

Komponent	Działa na
Konsola (aplikacja webowa)	Każda aktualna przeglądarka, pod adresem app.taleor.net lub na Państwa serwerze lokalnym
Konsola (aplikacja desktopowa)	Windows, macOS, Linux
Serwer lokalny, także w trybie izolowanym	Windows, macOS, Linux
Agent odtwarzacza	Windows, macOS, Linux, Raspberry Pi, Android
Odtwarzacz przeglądarkowy	Każda aktualna przeglądarka; parowanie za pomocą sześciocyfrowego kodu

Aplikacja desktopowa otwiera konsolę we własnym oknie, może odtwarzać eksponat na tym samym komputerze i zachowuje ostatnią poprawną konfigurację po ponownym uruchomieniu.

8.2 Sprzęt, w oparciu o otwarte standardy

taleor steruje sprzętem dowolnej marki za pomocą standardów, którymi ten sprzęt już się posługuje.

Rodzina	Przykłady	Protokoły
Wyświetlacze	Każdy ekran podłączony do komputera z odtwarzaczem taleor lub z odtwarzaczem przeglądarkowym	odtwarzacz taleor · odtwarzacz przeglądarkowy · HDMI
Projektory	Każdy projektor obsługujący PJLink; protokoły szeregowo właściwe dla danego producenta	PJLink · ESC/VP21 · RS-232 · TCP
Czujniki	Obecność, odległość (lidar, ultradźwięki), przycisk bezdotykowy, przycisk, RFID; kontrolery czujników podłączone do dowolnego odtwarzacza	Serial · USB · TCP
Kontrolery	Wejście OSC z konsoli oświetleniowej lub kontrolera pokazu, wyjście OSC z wyzwalacza, klawisze USB, pedały i płytki szeregowo, pilot ręczny	OSC · USB · serial
Dźwięk	Sieciowe procesory audio i głośniki, od zestawu słuchawkowego przy jednym ekspozycie po całą salę	REST · TCP
Oświetlenie	Oświetlenie architektoniczne i oświetlenie eksponatów	DALI

Pełna lista standardów: PJLink · RS-232 · TCP · DALI · MQTT · OSC · REST · WebSocket · serial · USB.

Sterowniki są dostępne dla tych rodzin urządzeń, a przed otwarciem obiektu testujemy je z Państwa sprzętem; potwierdzamy to na piśmie, zamiast przedstawiać listę logotypów. Jeśli urządzenie nie jest obsługiwane, zestaw do tworzenia sterowników pozwala integratorowi napisać własny: manifest, adapter, podpis. Producenci mogą przekazać nam urządzenie, a my opracujemy jego integrację.

8.3 Co to oznacza dla uzależnienia od dostawcy

Warstwa sterowania posługuje się otwartymi standardami, więc sprzęt nie jest związany z taleor. Serwer działa na Państwa własnym komputerze z własną bazą danych, więc dane nie są związane z naszą chmurą. Treści to zwykłe pliki multimedialne, a konfigurację eksportuje się jako zwykłe dane, więc obiekt, który rezygnuje, zabiera ze sobą swoje treści i swoją historię. Media mogą też pozostać na Dysku Google obiektu: taleor odczytuje tylko wybrane pliki, a ekrany przechowują kopię do odtwarzania offline. Wolimy, by klienci zostawali z nami dlatego, że produkt jest dobry, a nie dlatego, że odejście jest niemożliwe.

9 Modele wdrożenia i sposób oceny

9.1 Trzy modele

Chmura. Najszybszy start: otworzyć `app.taleor.net`, utworzyć obiekt, zainstalować agenta na każdym komputerze eksponatu. Agenci nawiązują połączenia wychodzące; nic nie łączy się z zewnątrz. Dla obiektów bez infrastruktury serwerowej oraz dla integratorów zarządzających kilkoma obiektami.

Serwer lokalny. Pakiet serwera na komputerze w budynku, z internetem lub bez niego. Dla instytucji z własnym działem IT oraz dla każdego obiektu, którego zasady zamówień wymagają przechowywania danych na miejscu.

Tryb izolowany. Serwer lokalny całkowicie bez dostępu do internetu; aktualizacje dostarcza personel. Dla obiektów o rygorystycznych zasadach sieciowych lub bez niezawodnego połączenia oraz dla wszystkich, którzy zdecydowali, że ich galerie nie powinny zależeć od połączenia, nad którym nie mają kontroli.

Wszystkie trzy modele korzystają z tego samego oprogramowania i tej samej konsoli, a wybór można później zmienić.

9.2 Lista kontrolna dla komisji przetargowych

Te pytania warto zadać każdemu dostawcy. Nasze odpowiedzi wraz z odpowiednim punktem:

Pytanie	taleor	Gdzie
Jak każdy odtwarzacz potwierdza swoją tożsamość? Czy używany jest wspólny klucz lub hasło?	Certyfikat dla każdego odtwarzacza; klucz generowany na komputerze, nigdy nie kopiowany; jeden urządzenie certyfikacji na obiekt	5.1
Czy połączenie z odtwarzaczem jest szyfrowane i uwierzytelniane w obu kierunkach? Czy certyfikaty mogą być wymieniane bez wizyty na miejscu?	TLS 1.3; wzajemny TLS; certyfikaty ważne 398 dni odnawiają się przez własne połączenie odtwarzacza	5.2
Czy sterowniki są podpisane? Czy aktualizacje są weryfikowane przed instalacją?	Sterowniki podpisane Ed25519, niepodpisane są odrzucane; suma kontrolna SHA-256 weryfikowana na odtwarzaczu	5.3
Czy wadliwa aktualizacja może wyłączyć eksponat?	Instalacja poza godzinami otwarcia; wycofanie i blokada po nieudanej kontroli stanu	5.3

Pytanie	taleor	Gdzie
Czy technik może zrestartować ekran, nie mając możliwości jego usunięcia?	Pięć ról; tak	5.4
Czy każde działanie jest powiązane z osobą, czasem i adresem? Czy administrator może skrócić lub wymazać dziennik?	Tak; eksport CSV; minimalny okres przechowywania 180 dni; usunięcie danych pozostawia znacznik usunięcia, a nie lukę	5.5
Co system rejestruje na temat zwiedzających i jak długo?	Obiekt, urządzenie, strefa, stan, czas; brak identyfikatora, co wymusza test schematu; okres przechowywania dla każdej klasy, usuwanie potwierdzone zapisem	5.6
Czy istnieje funkcja alarmu i jaki ma zasięg?	Obiekt, piętro, strefa lub wybrane odtwarzacze; pełny ekran; dźwięk eksponatów wyciszony	5.7
Czy cały system może działać lokalnie, bez internetu?	Tak; serwer lokalny i tryb izolowany	5.8, 9.1
Co dzieje się z eksponatami, gdy serwer jest niedostępny?	Odtwarzacze nadal odtwarzają z lokalnej pamięci podręcznej, także po ponownym uruchomieniu	5.9
Czy produkt przeszedł przegląd bezpieczeństwa i czy możemy zobaczyć ustalenia?	Tak; model zagrożeń, proof of concept, skanery, zweryfikowane poprawki	5.10
Jeśli konfiguracja jest zautomatyzowana, czy człowiek zatwierdza każdą konkretną zmianę we własnym imieniu?	Tak; propozycja, przegląd, zastosowanie; w dzienniku audytu jako zastosowane w imieniu wskazanej osoby	6.2
Jakie platformy i standardy sprzętowe?	Odtwarzacze na systemach Windows, macOS, Linux, Raspberry Pi, Android i w każdej przeglądarce; PJLink, RS-232, TCP, DALI, MQTT, OSC, REST, WebSocket, łącznie szeregowo, USB	8
Co pozostaje nasze, jeśli zrezygnujemy?	Treści jako zwykłe pliki, konfiguracja jako zwykłe dane, baza danych na Państwa komputerze	8.3

9.3 O co prosić w ramach pilotażu

Dokument to nie produkt. Warto poprosić o pilotaż obejmujący kilka eksponatów, który sprawdzi zabezpieczenia w praktyce: zarejestrować odtwarzacz z wzajemnym TLS i obejrzeć jego certyfikat; spróbować podłączyć drugi komputer

z kopią jego konfiguracji i potwierdzić, że zostanie odrzucony; poprosić kierownika technicznego, by zrestartował ekran, a następnie spróbował go usunąć; poprosić asystenta o zaproponowanie wyzwalacza, odrzucić propozycję, następnie zatwierdzić kolejną i przeczytać dziennik audytu; odłączyć kabel sieciowy i obserwować, jak odtwarzacz nadal odtwarza; wyeksportować dziennik audytu i potwierdzenie emisji do CSV; poprosić o zapis ostatniego przebiegu usuwania danych po okresie przechowywania. Każdy z tych kroków zajmuje kilka minut i mówi komisji więcej niż jakakolwiek lista funkcji.

10 O taleor

taleor to bezpieczny, agentowy sposób prowadzenia obiektu wystawienniczego: jego treści, aplikacji interaktywnych, odtwarzaczy i sprzętu z jednej konsoli, w chmurze, na serwerze lokalnym lub w trybie całkowicie izolowanym. Służy muzeom, centrom nauki, centrom doświadczeń marki, obiektom dziedzictwa kulturowego i atrakcjom turystycznym oraz osobom, które nimi zarządzają i dokonują dla nich zakupów.

taleor zostanie wprowadzony na rynek w listopadzie 2026 roku. Aby uzgodnić pilotaż lub poprosić o kartę katalogową do przetargów w języku angielskim, niemieckim, niderlandzkim lub polskim, prosimy o kontakt pod adresem hello@taleor.net.

Źródła i weryfikacja

Każde twierdzenie techniczne w tym dokumencie opiera się na wskazanym źródle w kodzie, dokumentacji projektowej lub przeglądzie bezpieczeństwa taleor, odnotowanym w rejestrze twierdzeń, który wymienia każde twierdzenie, rozdział, w którym się pojawia, oraz plik, z którego pochodzi. Rejestr można otrzymać, pisząc na adres hello@taleor.net.

Publiczne źródła wykorzystane w rozdziale 2, z których żadne nie jest źródłem danych liczbowych: botnet Mirai z 2016 roku (szeroko udokumentowany, m.in. przez amerykańską agencję Cybersecurity and Infrastructure Security Agency); BSI IT-Grundschutz (Niemcy); Baseline Informatiebeveiliging Overheid (Holandia); dyrektywa (UE) 2022/2555, znana jako NIS2; oraz Baseline Requirements CA/Browser Forum w zakresie 398-dniowego okresu ważności certyfikatów.

