
Erlebnisorte sicher betreiben

Warum ein Museum, ein Science Center oder eine Markenerlebniswelt wie eine gut geführte IT-Landschaft betrieben werden sollte, und wie taleor das umsetzt: jedes Gerät identifiziert, jede Verbindung verschlüsselt, jede Änderung einer Person zugeordnet, jeder Besucher anonym.

Whitepaper · Oktober 2026 · Version 1.0

Für Direktionen, technische und IT-Leitungen, AV-Integratoren, Berater und Vergabegremien von Museen, Science Centern, Markenerlebniswelten, Kulturerbestätten und Besucherattraktionen.

taleor

Inhalt

1	Zusammenfassung	3
2	Das Problem: Ein Standort ist heute eine IT-Landschaft	3
3	Was ein Standort wirklich braucht	5
4	So funktioniert taleor	6
5	Sicher von Grund auf	8
6	Einrichtung durch einen Assistenten	13
7	Auswertungen: was ein Standort erfährt	14
8	Läuft überall, nutzt Ihre vorhandene Technik	15
9	Betriebsmodelle und ihre Bewertung	17
10	Über taleor	19
	Quellen und Nachweise	19

1 Zusammenfassung

Ein Erlebnisort war früher ein Gebäude mit einigen Bildschirmen. Heute ist er ein Netzwerk: Hunderte von Computern, Displays, Projektoren, Lautsprechern, Leuchten und Sensoren von einem Dutzend Herstellern, jedes Gerät mit eigener Firmware, einer Adresse und oft einem Passwort. Betrieben wird das Ganze von einem kleinen Team, das kein IT-Team ist.

Dieses Whitepaper vertritt die These, dass ein Standort so betrieben werden sollte wie eine gut geführte IT-Landschaft: jedes Gerät identifiziert, jede Verbindung verschlüsselt, jede Änderung einer Person zugeordnet, jedes Update verifiziert, jeder Besucher anonym. Abschnitt 3 formuliert sieben Grundsätze, die Abschnitte 4 bis 8 beschreiben, wie taleor sie erfüllt, und Abschnitt 9 schließt mit einer Checkliste, die ein Vergabegremium jedem Anbieter vorlegen kann, auch uns.

Mit taleor betreiben Sie einen Erlebnisort sicher und agentenbasiert: Inhalte, interaktive Anwendungen, Player und Hardware, alles aus einer Konsole. taleor ruht auf drei Säulen. Es ist von Grund auf sicher. Es wird von einem Assistenten eingerichtet, der keine Änderung ohne die Zustimmung einer namentlich benannten Person übernimmt. Und seine Auswertungen zeigen „nicht gemessen“ statt null. taleor läuft als Web-App, als Desktop-App für Windows, macOS und Linux und als lokaler Server in Ihrem eigenen Gebäude, auch vollständig ohne Internet (Air-Gap). Die Player laufen unter Windows, macOS, Linux, Raspberry Pi und Android. taleor steuert Medientechnik jeder Marke über offene Standards.

2 Das Problem: Ein Standort ist heute eine IT-Landschaft

2.1 Hunderte Geräte, Dutzende Marken, ein kleines Team

Zählen Sie die Computer in den Ausstellungsräumen eines heutigen Museums: einer hinter den meisten Exponaten, dazu vernetzte Displays, Projektoren, Audioprozessoren, Lichtsteuerungen, Sensoren, Lesegeräte und Taster. An einem Standort mittlerer Größe liegt die Zahl im unteren dreistelligen Bereich. Die Beispieldaten, mit denen taleor entwickelt wurde, sind einem typischen Regionalmuseum nachempfunden und umfassen 69 Exponate und 342 Geräte mit 49 Steuerprotokollen. Das ist ein gewöhnlicher Bestand.

Jeder Hersteller bringt sein eigenes Protokoll mit, sein eigenes Verwaltungswerkzeug und seine eigene Vorstellung davon, wie Updates funktionieren. Die Inhalte wechseln jede Saison. Das Team besteht meist aus zwei

bis fünf Personen, deren Stellen nie für die Verwaltung einer Geräteflotte und das Einspielen von Patches gedacht waren.

2.2 Sicherheitsrisiken

Vier Schwachstellen verstärken sich gegenseitig.

Standard-Zugangsdaten. Professionelle AV-Technik wird mit einer Verwaltungsoberfläche und einem Werkspasswort ausgeliefert, das selten geändert wird. Denn es auf zweihundert Geräten zu ändern, ist eine Woche Arbeit, für die niemand zuständig ist. Das Mirai-Botnetz übernahm 2016 Geräte, indem es eine kurze Liste von Werkspasswörtern durchprobierte. Die Medientechnik von Standorten ist davon nicht ausgenommen.

Ungepatchte Player. Der Computer hinter einem Exponat läuft oft noch mit dem Betriebssystem, mit dem er in Betrieb genommen wurde, denn ein Update bedeutet, das Exponat zu schließen. Ein ungepatchter Rechner im selben Netzwerk wie Ticketing und Gebäudeleittechnik ist ein Einfallstor. Die Regelwerke, an denen öffentliche Stellen in Deutschland, den Niederlanden und Polen gemessen werden (BSI IT-Grundschutz, die Baseline Informatiebeveiliging Overheid und die Pflichten aus NIS2), behandeln zeitnahes Patchen und die Inventarisierung aller IT-Komponenten als Basisanforderungen.

Gemeinsame Geheimnisse. Viele Steuerungssysteme authentifizieren einen Player mit einem Schlüssel in einer Konfigurationsdatei. Wer diese Datei lesen kann, kann sich als dieser Player ausgeben.

Abhängigkeit von der Cloud. Ein System, das stillsteht, sobald das Internet oder die Cloud des Anbieters ausfällt, hat den Single Point of Failure an eine Stelle verlagert, die der Standort nicht beheben kann. Für eine öffentliche Einrichtung ist das auch eine Frage der Beschaffung: Wer hält die Daten, nach welchem Recht, und was geschieht, wenn der Vertrag endet?

2.3 Ausfälle, blinde Flecken und Herstellerbindung

Ausfälle sind das sichtbarste Versagen und das am wenigsten gemessene. Um 10:00 friert ein Bildschirm ein, mittags erwähnt es ein Besucher, um 14:00 erfährt es der Techniker, und nirgends sind die vier verlorenen Stunden erfasst.

Die meisten Standorte zählen Besucher am Eingang und sonst nirgends. Sie können nicht sagen, an welchem Exponat Menschen stehen geblieben sind, wie lange, oder ob ein Film bis zum Ende angesehen wurde. Wo gemessen wird, geschieht das oft in einem separaten System, allzu oft mit Kameras, die Personen identifizieren.

Jedes Teilsystem kommt mit eigenem Anbieter und eigenem Vertrag. Wird ein Anbieter übernommen oder stellt er ein Produkt ein, lassen sich Inhalte für einen proprietären Player nicht übertragen, und Hardware, die nur mit einer bestimmten Steuerung spricht, wird zu Schrott. Ein Gremium sollte nicht fragen „Unterstützt dieser Anbieter unsere Hardware?“, sondern „Was würde uns noch gehören, wenn dieser Anbieter verschwände?“

3 Was ein Standort wirklich braucht

Diese Probleme wurden schon einmal gelöst, in der allgemeinen IT. Was bisher fehlte, ist ihre Übertragung auf die besondere Gestalt eines Erlebnisorts: viele kleine Computer, viele Marken, ein kleines Team, ein öffentliches Publikum und ein Gebäude, das um 10:00 öffnen muss. Wir schlagen sieben Grundsätze vor.

1. **Jedes Gerät hat eine Identität, die sich nicht kopieren lässt.** Ein Schlüssel, der auf der eigenen Hardware erzeugt wurde und sie nie verlassen hat. Kein Passwort. Kein Token in einer Datei.
2. **Jede Verbindung ist verschlüsselt und in beide Richtungen authentifiziert.** Alles darunter erlaubt einem Fremden im Netzwerk des Standorts, eine überzeugende Fälschung aufzusetzen.
3. **Auf einem Player läuft nichts, was nicht vorher verifiziert wurde.** Treiber und Updates werden auf dem Player selbst anhand einer Signatur oder einer Prüfsumme geprüft, nicht nur an der Quelle.
4. **Jede Änderung hat einen Namen und eine Uhrzeit.** Ein Prüfpfad, den ein Administrator auf einen Tag kürzen oder bearbeiten kann, ist kein Prüfpfad.
5. **Jede Person erhält die Berechtigungen, die ihre Aufgabe erfordert, und nicht mehr.** Ein Facility Manager kann einen eingefrorenen Bildschirm neu starten, ohne ihn löschen zu können.
6. **Besucher bleiben konstruktionsbedingt anonym, nicht aufgrund einer Richtlinie.** Eine Eigenschaft des Datenbankschemas, die getestet wird.
7. **Das System gehört dem Standort.** Er kann alles im eigenen Gebäude betreiben, ohne Internet, und kann wechseln, ohne seine Inhalte zu verlieren.

Das würde jede kompetente IT-Abteilung von einer Flotte aus zweihundert Computern verlangen. Der Rest dieses Whitepapers beschreibt, wie taleor diese Grundsätze erfüllt.

4 So funktioniert taleor

4.1 Die Bestandteile

Die Konsole. Eine Web-App, in der das Personal jedes Exponat, jeden Player und die gesamte Medientechnik sieht, Inhalte lädt, Zeitpläne und Auslöser festlegt, Zustand und Störungen im Blick behält und die Auswertungen liest. Sie läuft in jedem aktuellen Browser oder als Desktop-App für Windows, macOS und Linux.

Der Player-Agent. Ein kleiner Hintergrunddienst auf dem Computer hinter jedem Exponat. Er hält eine dauerhafte, gegenseitig authentifizierte Verbindung zum Server, spielt ab, was ihm aufgetragen wird, steuert die Medientechnik an diesem Computer, liest dessen Sensoren aus, meldet seinen Zustand und hält sich selbst aktuell. Standardmäßig hält er eine lokale Kopie seiner Inhalte von 4 GB vor und spielt weiter, wenn der Server nicht erreichbar ist. Agents laufen unter Windows, macOS, Linux, Raspberry Pi und Android. Ein Bildschirm ohne Computer wird als Browser-Player gekoppelt, mit einem sechsstelligen Code, den man direkt vom Bildschirm abliest.

Treiber. Ein signiertes Paket, das taleor mitteilt, was ein Gerät der Medientechnik kann und wie es angesprochen wird. Die Konsole fordert einen Befehl an, etwa Strom, Quelle oder Lautstärke; der Treiber spricht das Protokoll.

Der Server. Die Datenbank, die WebSocket-Hubs für den Live-Status, die Zertifizierungsstelle für jeden Standort, der Medienspeicher, die Zeitplan-Engine, die Störungsüberwachung, das Audit-Protokoll und die Auswertungen. Es ist dieselbe Software in unserer Cloud oder auf einem Rechner in Ihrem Gebäude, mit oder ohne Internet.

4.2 Eine Software, drei Betriebsarten

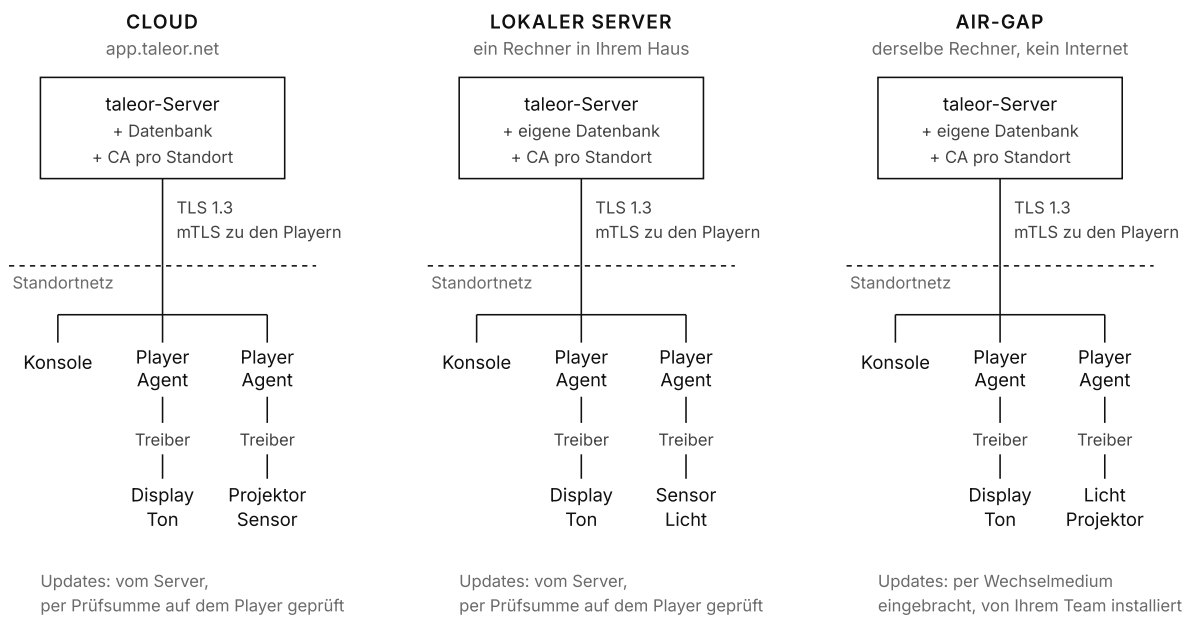


Abbildung 1. Eine Software, drei Betriebsarten. Derselbe Server, dieselbe Konsole und dieselben Player-Agents in der Cloud, auf einem lokalen Server im Gebäude oder als Air-Gap ohne Internet.

Im Cloud-Betrieb liegen Konsole und Server unter app.taleor.net, und die Agents bauen die Verbindung dorthin von sich aus auf; die Medientechnik im Netzwerk des Standorts wird von den Agents innerhalb dieses Netzwerks gesteuert. Im Betrieb mit lokalem Server wird dasselbe Paket auf einem Windows-, macOS- oder Linux-Rechner im Gebäude installiert, mit eigener privater Datenbank und eigener Zertifizierungsstelle, sodass Konsole, Player, Medien und Audit-Protokoll vollständig im Haus bleiben. Im Air-Gap-Betrieb läuft dieser Server ganz ohne Internet: Laufzeitumgebung und Datenbank sind im Paket enthalten, bei der Installation wird nichts heruntergeladen, und Updates bringt Ihr eigenes Personal auf Wechselmedienträgern herein. Eine Codebasis, eine Konsole; ein Standort, der in der Cloud beginnt, kann ins eigene Haus wechseln.

5 Sicher von Grund auf

5.1 Identität: ein Schlüssel, der den Rechner nie verlässt

taleor ersetzt das gemeinsame Geheimnis durch ein Zertifikat. Bei der Registrierung erzeugt ein Player auf seinem eigenen Rechner ein asymmetrisches Schlüsselpaar und sendet nur den öffentlichen Teil in einer Zertifikatsanforderung an die Zertifizierungsstelle des Standorts. Diese signiert ein Zertifikat und sendet es zurück. Der private Schlüssel wird nie übertragen. Von da an weist der Player seine Identität bei jedem TLS-Handshake durch eine live erzeugte Signatur nach. Es gibt nichts zu kopieren.

Eine Zertifizierungsstelle pro Standort, eingerichtet von einem Administrator in der Konsole. Eine Kompromittierung an einem Standort kann an keinem anderen Standort eine Identität erzeugen. Der private Schlüssel der Zertifizierungsstelle wird verschlüsselt gespeichert, mit einem Geheimnis, das von den übrigen Geheimnissen des Servers getrennt ist.

Der Anforderung wird nicht vertraut. Aus der Zertifikatsanforderung wird nur der öffentliche Schlüssel übernommen; Subject, Gültigkeitsdauer und alle Erweiterungen legt der Server fest. So kann ein Player weder den Namen eines anderen Players beanspruchen noch sich zur Zertifizierungsstelle machen. Player-Zertifikate werden ausschließlich für die Client-Authentifizierung ausgestellt, ein gestohlenes Zertifikat kann also keinen gefälschten Server vortäuschen.

Es gibt keine Schaltfläche „Zertifikat ausstellen“. Ein Zertifikat, dessen privaten Schlüssel der Server jemals besessen hat, würde den Zweck verfehlen.

5.2 Transport: verschlüsselt und geprüft, in beide Richtungen

Jede Verbindung zwischen Browser, Player und Konsole läuft über TLS 1.3 (für ältere Clients wird 1.2 akzeptiert). Player-Verbindungen nutzen gegenseitiges TLS (mTLS): Jede Seite legt der anderen ihr Zertifikat vor.

Ein gültiges Zertifikat ist notwendig, aber nicht hinreichend. Bei jeder Verbindung prüft der Server zusätzlich, und zwar gegen die Datenbank statt gegen eine zwischengespeicherte Liste, dass das Zertifikat weder widerrufen noch abgelaufen ist, dass das darin genannte Gerät noch existiert und dass das Gerät zu dem Standort gehört, für den das Zertifikat ausgestellt wurde.

Zertifikate gelten 398 Tage, die Obergrenze des CA/Browser Forum für öffentlich vertrauenswürdige Zertifikate, und werden in ihren letzten 30 Tagen über die eigene mTLS-Verbindung des Players erneuert. So tauscht eine Flotte ihre

Zugangsdaten aus, ohne dass jemand vor Ort sein muss. Mit der Ausstellung eines neuen Zertifikats wird das vorherige widerrufen.

Die Umstellung auf mTLS erfolgt schrittweise: Ein Übergangsmodus akzeptiert sowohl ein Zertifikat als auch die ältere Anmeldeinformation, während die Flotte Saal für Saal umzieht; sobald jeder Endpunkt ein Zertifikat hat, folgt der Pflichtmodus. Der Server verweigert diesen Wechsel, solange ein sich verbindendes Gerät ausgesperrt würde, denn die Alternative ist ein dunkles Museum. Wird der Modus wieder auf Aus gesetzt, ist die Umstellung sofort rückgängig gemacht.

5.3 Integrität: Nichts läuft, was nicht verifiziert wurde

Treiber sind signiert. Ein Treiber ist ein Paket mit einem Manifest und einer abgesetzten Ed25519-Signatur über den Hashwert des Pakets. Ein Produktivserver lehnt ein unsigniertes Paket standardmäßig ab, denn ein Treiber ist Code, der Sockets öffnet und mit Hardware kommuniziert. Integratoren und Hersteller können mit dem Treiber-Kit eigene Treiber schreiben und signieren.

Player-Updates werden per Prüfsumme verifiziert. Der Server veröffentlicht eine Version mit ihrer SHA-256-Prüfsumme. Der Player verifiziert die Prüfsumme vor allem anderen, entpackt das Update in ein Staging-Verzeichnis, tauscht es ein und startet neu. Schlägt die Verifizierung fehl, wird das Update abgelehnt.

Updates nehmen Rücksicht auf das Haus. Ein Update wird nur außerhalb der Öffnungszeiten installiert. Besteht eine neue Version ihre Funktionsprüfung nicht innerhalb von zehn Minuten, wird die vorherige Version wiederhergestellt und die neue für weitere Versuche gesperrt. Ein Standort kann einzelne Player von Updates ausnehmen; ein ausgenommener oder zurückliegender Player wird in der Konsole als „nicht aktuell“ markiert und gerät so nie unbemerkt in Vergessenheit.

5.4 Zugriff und Rollen

taleor kennt fünf zuweisbare Rollen.

Rolle	Wofür sie gedacht ist
Netzwerk-Admin	Alles, über alle Standorte der Organisation hinweg
Bereichs-Admin	Alle standortweiten Berechtigungen, über alle Standorte eines Unternehmensbereichs
Standort-Admin	Alle standortweiten Berechtigungen, an einem Standort
Redakteur	Inhalte, Reels, Zeitpläne und Vorlagen
Facility Manager	Bedienung der Medientechnik: Neustart, Strom, Quelle, Lautstärke

Die Rollen sind bewusst grob geschnitten, denn ein Berechtigungsmodell, das niemand erklären kann, wendet auch niemand an. Jeder Serverendpunkt prüft sowohl die Rolle als auch den Standort, sodass eine Person mit Rechten an einem Standort von einem anderen nichts sieht. Die Anmeldung erfolgt personenbezogen und wird nie geteilt; ein neues Konto muss sein Passwort bei der ersten Anmeldung ändern.

5.5 Der Prüfpfad

Jeder Schreibvorgang landet im Audit-Protokoll, mit Person, Aktion, Zeitpunkt und der Netzwerkadresse, von der er kam. Das gilt auch für Aktionen des Assistenten: Sie werden als vom Assistenten im Auftrag einer namentlich benannten Person übernommen protokolliert. Das Protokoll lässt sich in der Konsole filtern und mit denselben Filtern als CSV exportieren, sodass ein Prüfer es mitnehmen kann.

Zwei Eigenschaften schützen das Protokoll vor denen, die am meisten Kontrolle darüber haben. Für die Audit-Kategorie gilt eine erzwungene Mindestaufbewahrung von 180 Tagen: Ein Standort kann sein Protokoll länger aufbewahren, nie kürzer. Und wenn eine Person aus dem Personal ihr Recht auf Löschung ausübt, wird das Konto zu einem Platzhalter (Tombstone): Identität geschwärzt, Netzwerkadressen entfernt, Aktionen erhalten. So steht im Protokoll weiterhin, dass eine inzwischen gelöschte Person am Dritten eine Szene veröffentlicht hat. Ein Administrator kann sein eigenes Konto nicht löschen.

5.6 Datenschutz für Besucher, von Grund auf

Die Besucher eines Standorts sind Privatpersonen, viele davon Kinder. Richtig ist eine Gestaltung, bei der das System gar nicht erfassen kann, wer sie sind.

Die beiden Tabellen, die das Besucherverhalten enthalten, Präsenzereignisse und Interaktionsereignisse, speichern einen Standort, ein Gerät, eine Zone, ein Zustands- oder Ereigniswort und einen Zeitstempel. Sie enthalten keinerlei

Kennung der Person: keine Netzwerkadresse, kein Gesicht, kein Cookie, keine Sitzung. Das ist eine Eigenschaft des Schemas, kein Versprechen in einer Richtlinie; ein Test prüft das gegen die tatsächlichen Tabellendefinitionen und lässt den Build scheitern, sobald jemand eine solche Spalte hinzufügt.

Dahinter steht ein Verzeichnis von Verarbeitungstätigkeiten, das im Code liegt und in derselben Änderung geprüft wird wie der Code, der die Daten erzeugt: Zweck, Rechtsgrundlage, Grad der Identifizierbarkeit, Empfänger und Aufbewahrungsfrist für jede Datenkategorie. Eine nächtliche Bereinigung löscht Zeilen, deren Aufbewahrungsfrist abgelaufen ist, in Teilschritten, damit sie einen geöffneten Standort nie ausbremst, und schreibt für jeden Lauf eine Zeile, auch bei Fehlschlägen. Diese Dokumentation ist der Nachweis, nach dem ein Prüfer zuerst fragt.

Datenkategorie	Standard-Aufbewahrung	Untergrenze
Präsenz an einem Exponat	400 Tage	1 Tag
Berührungen und Auswahlen	400 Tage	1 Tag
Was wann abgespielt wurde	1825 Tage	365 Tage
Player-Protokolle	30 Tage	1 Tag
Wer was getan hat (Audit)	730 Tage	180 Tage

Die Maßnahmen sind nach den technischen Anforderungen von ISO/IEC 27701 umgesetzt, der Datenschutzerweiterung von ISO/IEC 27001. Mit dieser Aussage gehen wir sorgfältig um: Ein Produkt kann nicht nach 27701 zertifiziert werden; eine Organisation kann es, nach einem Audit. taleor setzt die Maßnahmen um, die die Norm technisch fasst, und erzeugt die Nachweise, die ein Prüfer braucht; die Einrichtung muss weiterhin eine verantwortliche Person für den Datenschutz benennen, ihre Datenschutz-Folgenabschätzung durchführen, ihre Verträge zur Auftragsverarbeitung abschließen und Hinweise in den Ausstellungsräumen anbringen.

5.7 Notfallnachricht

Ein einziges Bedienelement löst eine Notfallnachricht für den gesamten Standort, eine Etage, eine Zone oder ausgewählte Player aus. Die Nachricht füllt den ganzen Bildschirm, am unteren Rand läuft ein Hinweis, und der Ton der Exponate verstummt. Ein Player, der sich während einer Einblendung neu verbindet, erhält sie trotzdem. Die Notfallnachricht lässt sich von einem Handgerät des Personals

starten und beenden und wird wie jede andere Aktion protokolliert. Wir sagen bewusst „Ton der Exponate“: taleor bringt zum Schweigen, was es steuert, und ist keine Durchsage- oder Beschallungsanlage.

5.8 Isolation und Air-Gap

Das Paket für den lokalen Server installiert einen eigenen privaten PostgreSQL-Cluster, der nur auf der Loopback-Schnittstelle und auf einem Nicht-Standard-Port lauscht, sodass er nie auf eine bereits vorhandene Datenbank des Rechners trifft. Niemand tippt das Datenbankpasswort ein: Bei der Installation wird ein zufälliges erzeugt, das nur in einer Konfigurationsdatei steht, die das System und seine Administratoren lesen können. Eine Container-Laufzeitumgebung ist nicht erforderlich. Der Air-Gap-Betrieb ist dasselbe Paket ohne Internet (Abschnitt 4.2).

Die Medientechnik im Netzwerk des Standorts wird immer von innerhalb dieses Netzwerks gesteuert, durch die Player-Agents oder den lokalen Server. Die Cloud-Konsole braucht nie einen Zugang in Ihr Gebäude; die Agents bauen die Verbindung nach außen auf.

5.9 Sicheres Verhalten im Fehlerfall

- Ein Player, der die Verbindung zum Server verliert, spielt seine letzte funktionierende Konfiguration aus dem lokalen Cache weiter, auch über Neustarts hinweg, bis der Server wieder erreichbar ist.
- Fällt ein Player aus, wird eine Störung gemeldet: welcher Player, wo er steht, was er zeigen sollte und seit wann. Die Störung wird automatisch geschlossen, wenn der Player zurück ist; ein wiederholter Fehler aktualisiert die bestehende Störung.
- Der Server sichert seine Datenbank nach Zeitplan, mit fortlaufender Sicherungshistorie und Wiederherstellung von jedem Sicherungsstand. Alles, was aus der Inhaltsbibliothek gelöscht wird, lässt sich 30 Tage lang wiederherstellen.
- Der Server weigert sich, einen Standort auf mTLS festzulegen, solange ein Gerät außen vor bliebe; er lehnt einen veralteten Plan des Assistenten ebenso ab wie einen unsignierten Treiber. Zwischen Raten und Anhalten wählt taleor das Anhalten und sagt, warum.

5.10 Wie wir unsere eigene Arbeit prüfen

Vor dem Marktstart wurden Konsole, Player und Website von taleor einer Sicherheitsprüfung der Anwendung unterzogen: ein schriftliches Bedrohungsmodell, Proof-of-Concept-Exploits für jede vermutete Schwachstelle,

Scanner für Abhängigkeiten und statische Codeanalyse sowie ein erneuter Scan nach den Korrekturen. Jeder Befund hat einen Schweregrad, eine verantwortliche Person und eine verifizierte Korrektur; eine Prüfstufe gilt nicht als bestanden, solange ein blockierender Befund offen ist. Fordern Sie dasselbe von jedem Anbieter.

6 Einrichtung durch einen Assistenten

6.1 Was der Assistent tut

Ein interaktives Exponat einzurichten war schon immer Spezialarbeit, die am Standort nur eine Person beherrscht. taleor enthält in der Konsole einen Assistenten namens Oli. Sie schreiben, was Sie möchten:

Wenn jemand dem Bildschirm im Foyer näher als einen Meter kommt, zum Begrüßungsfilm wechseln, und zurück, wenn dreißig Sekunden lang niemand da ist.

Der Assistent liest den Standort aus (Exponate, Player, Reels, hinterlegte Eingänge) und schlägt einen Plan vor, in dem die genauen Änderungen aufgeführt sind:

Liest Bildschirm im Foyer: Präsenzsensoren hinterlegt, 2 Reels.
Schlägt vor: bei Abstand von 100 cm oder weniger „Begrüßungsfilm“ abspielen, nach 30 s zurück.
Wartet auf Ihre Prüfung.

Sie lesen den Plan. Sie wählen „Übernehmen“ oder „Verwerfen“. Fehlt etwas, sagt der Assistent, was fehlt: kein Reel namens „Begrüßungsfilm“ oder kein Präsenzsensoren an diesem Player. Ist eine Anfrage mehrdeutig, stellt der Assistent jeweils nur eine Frage, und er nimmt nie Hardware an, die nicht vorhanden ist.

Der Assistent schlägt Auslöser, Reel-Zuweisungen und das Aktivieren eines Auslösers vor und übernimmt sie, sobald Sie zustimmen. Jede Einstellung bleibt auch von Hand verfügbar.

6.2 Das Berechtigungsmodell

Der Assistent ist kein privilegierter Benutzer. Er hat keine eigenen Berechtigungen.

- **Lesen.** Seine Werkzeuge zum Betrachten des Standorts sind schreibgeschützt und auf den Standort beschränkt, in dem die Person gerade arbeitet.

- **Vorschlagen.** Seine Planungswerkzeuge zeichnen nur einen vorgeschlagenen Schritt auf. Es wird nichts ausgeführt. Das ist getestet.
- **Übernehmen.** Bei „Übernehmen“ laufen die gespeicherten Schritte durch dieselben Servicefunktionen, Validierungen und Berechtigungsprüfungen, als hätte die Person jede Änderung von Hand vorgenommen. Wer etwas nicht ändern darf, kann es also auch nicht vom Assistenten ändern lassen. Das Audit-Protokoll verzeichnet das Ergebnis als vom Assistenten für diese namentlich benannte Person übernommen.
- **Veraltete Pläne.** Ein Plan, der veraltet ist, weil zwischen Vorschlag und Zustimmung ein Reel gelöscht wurde, wird abgelehnt, statt dass geraten wird.
- **Begrenzung.** Der Assistent ist ausgeschaltet und ausgeblendet, solange er nicht konfiguriert ist. Seine Nutzung wird gemessen, mit einer festen monatlichen Obergrenze für den gesamten Server. Fehlermeldungen des zugrunde liegenden Dienstes werden nie wörtlich angezeigt.

6.3 Warum erst prüfen, dann übernehmen

Ein System, das ändert, was auf zweihundert Bildschirmen läuft, muss die Frage beantworten können: „Wer hat das geändert, und hat ein Mensch zugestimmt?“ Stellen Sie diese Frage jedem Produkt, das mit automatischer Einrichtung wirbt.

7 Auswertungen: was ein Standort erfährt

7.1 Auf Basis dessen, was die Player tatsächlich melden

Die Auswertungen von taleor, in der Konsole „Statistiken“ genannt, beruhen auf dem, was Player und Sensoren melden, nicht auf einem separaten Zählsystem: Der Sensor, der einen Film startet, ist derselbe Sensor, der zählt, wie viele Menschen stehen geblieben sind und wie lange. Jede Kennzahl lässt sich auf den gesamten Standort, eine Etage, eine Zone oder einen Player beziehen, für heute, diese Woche, diesen Monat oder dieses Jahr, jeweils mit dem vorherigen Zeitraum zum Vergleich.

7.2 Was Sie sehen

Besuchersfrequenz und Verweildauer. Besucher pro Stunde, Tag oder Monat, aus Sensoren und Touch-Eingaben. Durchschnittliche Verweildauer bei engagierten Besuchen. Die meistbesuchten Zonen und Uhrzeiten, als Heatmap nach Zone und Stunde.

Was am besten funktioniert hat. Exponate, sortiert nach Besuchen und Verweildauer, sodass eine wenig beachtete Ecke auffällt, noch bevor ein Kurator daran vorbeikommt. Besucher und Verweildauer gehören zum Exponat, Betriebszeit und Wiedergaben zum jeweiligen Player.

Wiedergabenachweis. Jedes Element, jede Wiedergabe, vollständig abgespielt oder nicht, mit einem CSV-Export, der denselben Bereich und Zeitraum berücksichtigt. Standardmäßig fünf Jahre aufbewahrt, sodass er eine Lizenzlaufzeit und einen Sponsoringvertrag überdauert.

Player-Zustand und Verfügbarkeit. Verfügbarkeit pro Player im gewählten Zeitraum, ermittelt aus Zustandsmeldungen. Gibt es in einem Zeitraum keine Zustandsmeldungen, wird das als unbekannt angezeigt, nicht als in Ordnung.

7.3 Ehrliche Zahlen

Eine Kennzahl, die nicht gemessen werden kann, zeigt „nicht gemessen“, nie null. Eine Zone ohne Sensor meldet nicht null Besucher; sie meldet, dass die Besucherzahl dort nicht gemessen wurde.

7.4 Auch hier: Datenschutz von Grund auf

Die Ereignisse hinter jeder Kennzahl sind die aus Abschnitt 5.6, ohne Kennung der Besucher: keine Kameras, keine Gesichtsdetektion, kein Geräte-Tracking, keine Cookies.

8 Läuft überall, nutzt Ihre vorhandene Technik

8.1 Plattformen

Komponente	Plattform
Konsole (Web-App)	Jeder aktuelle Browser, unter app.taleor.net oder auf Ihrem lokalen Server
Konsole (Desktop-App)	Windows, macOS, Linux
Lokaler Server, auch im Air-Gap-Betrieb	Windows, macOS, Linux
Player-Agent	Windows, macOS, Linux, Raspberry Pi, Android
Browser-Player	Jeder aktuelle Browser; Kopplung mit sechstelligem Code

Die Desktop-App öffnet die Konsole in einem eigenen Fenster, kann das Exponat auf demselben Computer abspielen und behält die letzte funktionierende Konfiguration über einen Neustart hinweg.

8.2 Hardware, angebunden über offene Standards

taleor steuert Medientechnik jeder Marke über die Standards, die sie bereits spricht.

Gerätefamilie	Beispiele	Über
Displays	Jeder Bildschirm an einem Computer mit dem taleor Player oder mit dem Browser-Player	taleor Player · Browser-Player · HDMI
Projektoren	Jeder Projektor, der PJLink spricht; herstellerspezifische serielle Protokolle	PJLink · ESC/VP21 · RS-232 · TCP
Sensoren	Präsenz, Abstand (Lidar, Ultraschall), berührungsloser Taster, Taster, RFID; Sensorsteuerungen hinter jedem Player	Serial · USB · TCP
Steuerungen	OSC-Eingang von einem Lichtpult oder Showcontroller, OSC-Ausgang von einem Auslöser, USB-Tasten, Fußpedale und serielle Platinen, ein Handgerät	OSC · USB · serial
Ton	Vernetzte Audioprozessoren und Lautsprecher, vom Kopfhörer an einem Exponat bis zur ganzen Halle	REST · TCP
Licht	Architektur- und Exponatbeleuchtung	DALI

Alle Standards im Überblick: PJLink · RS-232 · TCP · DALI · MQTT · OSC · REST · WebSocket · seriell · USB.

Für diese Gerätefamilien gibt es Treiber, und wir testen sie vor Ihrer Eröffnung mit Ihrer Medientechnik; das halten wir schriftlich fest, statt eine Liste von Logos zu präsentieren. Ist ein Gerät nicht abgedeckt, kann ein Integrator mit dem Treiber-Kit selbst einen Treiber schreiben: ein Manifest, ein Adapter, eine Signatur. Hersteller können uns ein Gerät bringen, und wir bauen die Integration dafür.

8.3 Was das für die Herstellerbindung bedeutet

Die Steuerungsebene spricht offene Standards, daher ist die Hardware nicht an taleor gebunden. Der Server läuft auf Ihrem eigenen Rechner mit eigener Datenbank, daher sind die Daten nicht an unsere Cloud gebunden. Inhalte sind gewöhnliche Mediendateien, und die Konfiguration lässt sich als einfache Daten exportieren. Ein Standort, der geht, nimmt also seine Inhalte und seine Historie mit. Medien können auch im eigenen Google Drive des Standorts bleiben: taleor

liest nur die ausgewählten Dateien, und die Bildschirme halten eine Kopie für die Offline-Wiedergabe. Uns ist lieber, dass Sie bleiben, weil das Produkt gut ist, als weil ein Wechsel unmöglich wäre.

9 Betriebsmodelle und ihre Bewertung

9.1 Drei Modelle

Cloud. Der schnellste Einstieg: app.taleor.net öffnen, den Standort anlegen, den Agent auf jedem Exponat-Computer installieren. Die Agents bauen Verbindungen nach außen auf; von außen wird keine Verbindung aufgebaut. Für Standorte ohne eigene Serverinfrastruktur und für Integratoren, die mehrere Standorte betreuen.

Lokaler Server. Das Serverpaket auf einem Rechner im Gebäude, mit oder ohne Internet. Für Einrichtungen mit eigener IT und für jeden Standort, dessen Beschaffungsregeln verlangen, dass die Daten im eigenen Haus bleiben.

Air-Gap. Der lokale Server ganz ohne Internet; Updates bringt das Personal herein. Für Häuser mit strengen Netzwerkrichtlinien oder ohne zuverlässige Anbindung und für alle, die entschieden haben, dass ihre Ausstellungen nicht von einer Verbindung abhängen sollen, die sie nicht selbst kontrollieren.

Alle drei nutzen dieselbe Software und dieselbe Konsole, und die Wahl lässt sich später ändern.

9.2 Eine Checkliste für Vergabegremien

Stellen Sie diese Fragen jedem Anbieter. Unsere Antworten, mit dem jeweiligen Abschnitt:

Frage	taleor	Abschnitt
Wie weist jeder Player seine Identität nach? Ist ein gemeinsamer Schlüssel oder ein Passwort im Spiel?	Zertifikat pro Player; Schlüssel auf dem Rechner erzeugt, nie kopiert; eine Zertifizierungsstelle pro Standort	5.1
Ist die Player-Verbindung verschlüsselt und in beide Richtungen authentifiziert? Lassen sich Zertifikate ohne Besuch vor Ort erneuern?	TLS 1.3; mTLS; Zertifikate mit 398 Tagen Laufzeit erneuern sich über die eigene Verbindung des Players	5.2
Sind Treiber signiert? Werden Updates vor der Installation verifiziert?	Ed25519-signierte Treiber, unsignierte werden abgelehnt; SHA-256-Prüfsumme wird auf dem Player verifiziert	5.3

Frage	taleor	Abschnitt
Kann ein fehlerhaftes Update ein Exponat lahmlegen?	Installation außerhalb der Öffnungszeiten; bei fehlgeschlagener Funktionsprüfung Rückkehr zur vorherigen Version und Sperre	5.3
Kann ein Techniker einen Bildschirm neu starten, ohne ihn löschen zu können?	Fünf Rollen; ja	5.4
Ist jede Aktion mit Person, Zeitpunkt und Adresse versehen? Kann ein Administrator das Protokoll kürzen oder löschen?	Ja; CSV-Export; Mindestaufbewahrung 180 Tage; eine Löschung hinterlässt einen Platzhalter, keine Lücke	5.5
Was erfasst das System über Besucher, und wie lange?	Standort, Gerät, Zone, Zustand, Zeitpunkt; keine Kennung, durch einen Schematest erzwungen; Aufbewahrung je Kategorie, Löschung nachgewiesen	5.6
Gibt es eine Notfallnachricht, und was erreicht sie?	Standort, Etage, Zone oder ausgewählte Player; ganzer Bildschirm; Ton der Exponate stumm	5.7
Kann das gesamte System im eigenen Haus laufen, ohne Internet?	Ja; lokaler Server und Air-Gap	5.8, 9.1
Was geschieht mit den Exponaten, wenn der Server nicht verfügbar ist?	Die Player spielen aus dem lokalen Cache weiter, auch über Neustarts hinweg	5.9
Wurde das Produkt einer Sicherheitsprüfung unterzogen, und können wir die Befunde einsehen?	Ja; Bedrohungsmodell, Proofs of Concept, Scanner, verifizierte Korrekturen	5.10
Wenn die Einrichtung automatisiert ist: Stimmt eine Person jeder konkreten Änderung zu, in ihrem Namen?	Ja; vorschlagen, prüfen, übernehmen; protokolliert als für die namentlich benannte Person übernommen	6.2
Welche Plattformen und Hardware-Standards?	Player unter Windows, macOS, Linux, Raspberry Pi, Android und in jedem Browser; PJLink, RS-232, TCP, DALI, MQTT, OSC, REST, WebSocket, seriell, USB	8
Was gehört uns, wenn wir gehen?	Inhalte als gewöhnliche Dateien, Konfiguration als einfache Daten, die Datenbank auf Ihrem Rechner	8.3

9.3 Was Sie in einem Pilotprojekt verlangen sollten

Ein Papier ist kein Produkt. Verlangen Sie ein Pilotprojekt mit einigen Exponaten, in dem die Schutzmechanismen auf die Probe gestellt werden: einen Player mit mTLS registrieren und sein Zertifikat prüfen; einen zweiten Rechner mit einer Kopie seiner Konfiguration ausprobieren und bestätigen, dass er abgewiesen wird; einen Facility Manager einen Bildschirm neu starten und anschließend versuchen lassen, ihn zu löschen; den Assistenten einen Auslöser vorschlagen lassen, den Vorschlag verwerfen, dann einem Vorschlag zustimmen und das Audit-Protokoll lesen; ein Netzkabel ziehen und beobachten, wie der Player weiterspielt; Audit-Protokoll und Wiedergabenachweis als CSV exportieren; den Nachweis des letzten Bereinigungslaufs anfordern. Jeder Schritt dauert Minuten und sagt einem Gremium mehr als jede Funktionsliste.

10 Über taleor

Mit taleor betreiben Sie Erlebnisorte sicher und agentenbasiert: Inhalte, interaktive Anwendungen, Player und Hardware, aus einer Konsole, in der Cloud, auf einem lokalen Server oder vollständig ohne Internet. taleor richtet sich an Museen, Science Center, Markenerlebniswelten, Kulturerbestätten und Besucherattraktionen und an die Menschen, die sie betreiben und für sie beschaffen.

talor startet im November 2026. Schreiben Sie an hello@taleor.net, um ein Pilotprojekt zu vereinbaren oder das Datenblatt für Ausschreibungen auf Englisch, Deutsch, Niederländisch oder Polnisch anzufordern.

Quellen und Nachweise

Jede technische Aussage in diesem Whitepaper beruht auf einer benannten Quelle im Code, in den Designdokumenten oder in der Sicherheitsprüfung von taleor. Sie ist in einem Aussagenregister erfasst, das jede Aussage, den Abschnitt, in dem sie steht, und die Datei, aus der sie stammt, aufführt. Schreiben Sie an hello@taleor.net, um das Register zu erhalten.

Öffentliche Referenzen in Abschnitt 2, jeweils ohne Zahlenangaben: das Mirai-Botnetz von 2016 (umfassend dokumentiert, unter anderem von der US-Behörde Cybersecurity and Infrastructure Security Agency); BSI IT-Grundschutz (Deutschland); die Baseline Informatiebeveiliging Overheid (Niederlande); die Richtlinie (EU) 2022/2555, bekannt als NIS2; sowie die Baseline Requirements des CA/Browser Forum für die Zertifikatslaufzeit von 398 Tagen.

