XIENT.

XIENT STANDORTBESTIMMUNG · PRAXISFALL

Das Standortbild in der Praxis. Geheimhaltung sicher absichern, bevor outgesourct wird.

Ein realer Xient-Fall, anonymisiert dargestellt - nachgezeichnet im Format des heutigen Xient Executive Assessments: Entscheidungsfrage, Vorgehen, Befunde, Nachweis, Ergebnis.

Kunde: Technologiekonzern (DAX) · **Umfeld:** zentrales SAP-BW-Reporting, täglich Millionen neuer Datensätze

Anlass: geplante Übergabe des Supports an einen externen Dienstleister · **Schutzgut:** vertraulich klassifizierte Daten (VS-NfD)

> Anonymisierte, verfremdete und um exemplarische Detailtiefe ergänzte Darstellung eines realen Projekts. Konkrete Systeminterna, Namen und vertrauliche Inhalte sind weder genannt noch rekonstruierbar; die dargestellten Prüffelder und Mechanismen entsprechen dem üblichen Vorgehen in Fällen dieser Art.

AUSGANGSLAGE

Die Entscheidungsfrage.

Der Konzern wollte den Support eines zentralen SAP-BW-Reportings an einen externen Dienstleister übergeben - ein üblicher, betriebswirtschaftlich sinnvoller Schritt. Im System lagen jedoch streng vertrauliche, einer Geheimhaltungsstufe unterliegende Daten (VS-NfD). Für diese gilt keine Risikoabwägung nach Augenmaß, sondern ein hartes Kriterium: kein unbefugter Zugriff, in keinem Szenario.

Die Entscheidungsfrage

Kann der Support übergeben werden, ohne dass VS-NfD-relevante Daten einsehbar werden - und was muss vor der Übergabe nachweisbar sichergestellt sein?

Das Wort „nachweisbar" trägt hier die Last: Bei diesem Schutzanspruch zählt nicht das gute Konzept, sondern die lückenlose, belegbare Umsetzung. Schon die kleinste Einsehbarkeit wäre inakzeptabel gewesen.

> **„Zuverlässigkeit und Perfektion waren für die Zusammenarbeit essenziell."**
>
> IT-Manager des Auftraggebers

VORGEHEN

Vier Phasen - vom Schutzbedarf zur Übergabefähigkeit.

1 · Auftragsklärung: Abstimmung mit IT, Fachbereich und den für den Geheimschutz Verantwortlichen; Festlegung von Schutzgut, Prüfumfang und Abnahmekriterien. Zentrale Vorentscheidung: Der Nachweis sollte nicht auf Aussagen beruhen, sondern auf systemischer Ortung.

2 · Assessment: Analyse der Datenverteilung im BW, des Berechtigungskonzepts, der nachgelagerten Verteilwege und der Betriebsprozesse - Interviews plus technische Tiefenprüfung.

3 · Expertenkonsolidierung: Data-Analytics-, BI- und Security-Perspektive zu einem Befund zusammengeführt; Lösungsweg gegen die Betriebsrealität eines Massendaten-Systems geprüft.

4 · Entscheidung und Umsetzung: Freigabe des hybriden Lösungswegs, Umsetzung in ABAP, Nachweisführung, Abnahme - erst danach die Support-Übergabe.

PRÜFFELDER

Was untersucht wurde - und warum.

Sechs Prüffelder, ein Prinzip: Schutz ist nur dann belegbar, wenn jeder Weg betrachtet wird, auf dem klassifizierte Information sichtbar werden kann - nicht nur der offensichtliche.

Prüffeld	Leitfrage	Ausgangsbefund	Status nach Projekt
Datenverteilung im BW	Wo überall liegen VS-NfD-relevante Daten - auch historisch?	Relevante Daten über viele Ablageorte verstreut, darunter bislang unbekannte Bereiche	vollständig geortet
Ladeschichten und Zwischenspeicher	Bleiben Schutzdaten in Eingangs- und Zwischenschichten liegen?	Historische Ladebestände enthielten schutzrelevante Sätze außerhalb der Reporting-Sicht	bereinigt und geregelt
Berechtigungskonzept	Trennen die Rollen sauber zwischen Arbeitsfähigkeit und Einsicht?	Rollen historisch gewachsen, nicht auf eine Support-Übergabe zugeschnitten	neu zugeschnitten
Nachgelagerte Verteilwege	Verlassen Schutzdaten das System über Berichte, Exporte, Verteilungen?	Einzelne Verteilwege waren nicht auf Klassifizierung geprüft	geprüft und geschlossen
Test- und Kopiersysteme	Tragen QA- und Testumgebungen produktive Schutzdaten?	Kopierprozesse ohne Rücksicht auf Klassifizierung angelegt	Regeln etabliert
Betrieb und Protokollierung	Ist ausnahmsweiser Zugriff geregelt, protokolliert, auswertbar?	Ausnahmezugriffe möglich, aber nicht durchgängig nachvollziehbar	protokolliert

Die Prüffelder sind zur Anonymisierung verallgemeinert; Zuschnitt und Tiefe folgen dem realen Projekt.

Vier Kernbefunde - und was daraus wurde.

BEFUND 1 **kritisch vor Übergabe**

Die schützenswerten Daten lagen verstreuter, als bekannt war.

Beobachtung	VS-NfD-relevante Informationen konnten an vielen Orten im BW liegen - in aktiven Datenzielen ebenso wie in historischen Beständen. Der eigens entwickelte Suchalgorithmus deckte auch Bereiche auf, die intern niemand mehr auf der Karte hatte.
Bewertung	Das ist der Normalfall gewachsener Landschaften, kein Versäumnis Einzelner: Über Jahre wandern Daten in Strukturen, die später niemand mehr vollständig überblickt. Ohne vollständige Ortung wäre jede Berechtigungslösung Stückwerk geblieben.
Lösung	Systemische Ortung statt Befragung: präzise Analyse-Algorithmen, die jeden potenziellen Ablageort zuverlässig finden und das Ergebnis reproduzierbar machen - die Grundlage für alles Weitere.

BEFUND 2 **methodisch entscheidend**

Der naheliegende Ansatz hätte das System gefährdet.

Beobachtung	Ein rein algorithmischer Eingriff in ein System mit täglich Millionen neuer Datensätze hätte Ladeketten, Laufzeiten und damit die Integrität des produktiven Reportings riskiert.
Bewertung	Sicherheitsmaßnahmen, die den Betrieb gefährden, sind keine Lösung - sie werden umgangen oder zurückgebaut. Die Bewertung muss Technik und Betriebsrealität zusammen denken.
Lösung	Hybrider Weg: Die Algorithmen orten und klassifizieren; ein neues, maßgeschneidertes Berechtigungskonzept setzt den Schutz durch - vollständig in ABAP umgesetzt, im Takt des Systems statt gegen ihn.

BEFUND 3 organisatorisch

Sicherheit und Arbeitsfähigkeit mussten zusammen gelöst werden.

Beobachtung	Das externe Support-Team braucht echten, breiten Systemzugriff für die tägliche Arbeit - Monitoring, Fehleranalyse, Ladeketten, Transporte.
Bewertung	Ein Konzept, das den Support faktisch arbeitsunfähig macht, scheitert an der Realität - und provoziert genau die informellen Umgehungswege, die es verhindern soll.
Lösung	Rollenzuschnitt entlang der tatsächlichen Support-Tätigkeiten: voller technischer Zugriff auf Strukturen und Prozesse, konsequent getrennt von der inhaltlichen Einsicht in klassifizierte Daten.

BEFUND 4 nachhaltig

Einmal absichern reicht nicht - neue Daten kommen täglich.

Beobachtung	Mit täglich Millionen neuer Datensätze ist jede Stichtagslösung nach kurzer Zeit veraltet: Neue schutzrelevante Sätze entstehen laufend.
Bewertung	Der Schutz muss als dauerhafter Mechanismus angelegt sein, nicht als Projektergebnis - sonst beginnt die Erosion am Tag nach der Abnahme.
Lösung	Die Ortungs- und Schutzlogik läuft als wiederholbarer Prozess im System weiter; neue Bestände werden erfasst, das Berechtigungskonzept greift automatisch.

NACHWEIS

Wie „lückenlos" belegt wurde.

- **Reproduzierbare Ortung:** Die Suchergebnisse waren wiederholbar und vollständig dokumentiert - keine Einzelmeinung, sondern ein prüfbarer Systembefund.
- **Negativtests:** Mit den neuen Support-Rollen wurde aktiv versucht, klassifizierte Inhalte einzusehen - über Berichte, Datenvorschau und Ausnahmewege. Ergebnis: kein Zugriff.
- **Positivtests:** Dieselben Rollen wurden gegen den Support-Alltag geprüft - alle Arbeitsszenarien blieben vollständig möglich.
- **Abnahme:** Freigabe durch die fachlich und für den Geheimschutz Verantwortlichen - erst danach die Übergabe an den Dienstleister.

ERGEBNIS

Was geblieben ist.

- Die vertraulichen Informationen sind vollständig gegen unbefugten Zugriff geschützt - nachweisbar, nicht behauptet.
- Der Support konnte wie geplant übergeben werden; das Outsourcing-Vorhaben wurde nicht durch Sicherheit blockiert, sondern durch Sicherheit erst möglich.
- Das Support-Team arbeitet ohne Einschränkung - und ohne Einblick in Schutzdaten.
- Der Schutz läuft als dauerhafter Mechanismus weiter, nicht als abgeschlossene Einmalaktion.

Warum dieser Fall das Executive Assessment erklärt

Die Reihenfolge ist das Muster: erst die Lage vollständig verstehen (wo liegen die kritischen Daten wirklich - auch dort, wo niemand mehr hinschaut?), dann bewerten (was gefährdet den Betrieb, was schützt wirklich?), dann entscheiden, umsetzen und nachweisen. Genau diese Reihenfolge liefert heute das Xient Executive Assessment - vor Outsourcing-, Migrations- und KI-Entscheidungen.

Der Weg dorthin

Xient Executive Assessment - ab 30.000 Euro. Festpreis nach Scoping Session.
Unabhängig in der Bewertung und methodisch sowie kommerziell eigenständig.

Gespräch vereinbaren: xient.ai/unabhaengiges-gutachten · info@xient.de · +49 221 16533980

Xient GmbH · Werkstättenstraße 19 · 51379 Leverkusen · Anonymisierte, verfremdete und exemplarisch ergänzte Darstellung eines realen Xient-Projekts.