Big Data – Big Treasure!

Wie Sie Ihren Informationsschatz schützen

Neue Technologien und Services wie BI-Cloud-Services, Änderungen bei Gesetzen und Urteilen zum Datenschutz, im Widerspruch stehende gesetzliche Forderungen – wie bei Mindestaufbewahrungsfristen und Löschgeboten – und täglich neue Fälle von Datenpannen und Informationsdiebstahl verunsichern Unternehmen, wie BI-Daten richtig zu schützen sind.

BI ein Nibelungenhort

Das BI ist der zentrale Ort für Informationen im Unternehmen: Hier werden Daten aus verschiedenen Quellen im Unternehmen und von externen Partnern zusammengeführt. Aus den Daten werden kanonisierte, semantische Informationen und aus diesen werden aussagekräftige Erkenntnisse und insbesondere entscheidungsrelevante Informationen und Pläne.

Im BI findet sich die eine zentrale Wahrheit über Zustand und Entwicklung des gesamten Unternehmens, die Basis für Abweichungsanalysen zu den geschäftlichen Zielen und die Basis für neue Pläne und Business-Szenarien. Mithin ein großer Schatz für Ihr Unternehmen – und damit auch für andere Interessenten!

Ein Hort? – Es sind doch nur Daten!

Was passiert, wenn es passiert, zeigen folgende Szenarien.

- Der Schatz wird geraubt: Wenn es lediglich geschäftliche Informationen sind, sind bei Bekanntwerden im mildesten Falle ein signifikanter Reputationsschaden und in Folge ein Umsatzrückgang zu erwarten, im schlimmsten Fall Mitbewerber, die Wettbewerbsvorteile erkennen und ausbeuten. Wenn es sich um personenbezogene Daten handelt, stellen sich massive Reputationsschäden ein, weil alle potentiell Betroffenen informiert werden müssen und das so gut wie immer in die Presse gelangt (vgl Kreditkarten- und andere Identitäts-Diebstähle, vgl. Sony 2011 mit 75 Mio Betroffenen), dazu kommen strafrechtliche Konsequenzen vom Ordnungsgeld bis zur persönlichen Haftung des Managements. Wenn es sich um anvertraute Daten Dritter handelt (z.B. GfK oder Infratest), stehen Schadenersatzansprüche wegen Vermögensschäden insbesondere wegen IP-Rechtsverletzungen im Raum.
- Der Schatz geht verloren oder ist beschädigt: Ob durch interne oder externe Ursachen wie Vorsatz oder Katastrophe verursacht die Integrität der Informationen ist verletzt, d.h. es ist entweder kein Verlass mehr auf die vorhandenen Informationen oder sie sind vollständig verloren. Die Handlungs- und Entscheidungsfähigkeit des Unternehmens ist in der Folge erheblich eingeschränkt!

Anleitung zum Schutz des Horts

Die ISO 27001 wurde als Best Practice für Information Security (IS) für ganze Unternehmen oder wesentliche Prozesse entworfen, muss also für den Shared Service BI entsprechend in den Unternehmenskontext eingepasst werden. Im Zentrum der IS for BI stehen die schutzwürdigen Informationen und die Organisation, die mit ihnen umgeht. IS for BI ist daher nicht gleich IT-Security zu setzen, sondern die Summe aller technisch-organisatorischen Maßnahmen, die das BI angemessen schützen – IT-Security ist ein relevanter Teil davon.

Ausgehend von den Schutzzielen der ISO 27001 (siehe Kasten) ist der wesentliche Startpunkt zu einem angemessenen Schutz des BI (1) die Feststellung der Schutzwürdigkeit der Informationen und (2) die Ableitung der spezifischen Bedrohungen.

Der Wert des Horts

Die Schutzwürdigkeit des BI festzustellen, bedeutet folgende Fragen zu beantworten:

(1) Welche Kleinodien sind im BI? Anhand des semantischen Daten- bzw. Informationsmodells des BI aufgebaut wird das Informationen-Register als führende Struktur zur Bewertung der Schutzwürdigkeit genutzt.
(2) Wofür werden sie benötigt? Die Business Impact Analysis (BIA) eröffnet, für welche Zwecke die Informationen des BI benötigt werden und wie lange man ohne sie auskommen kann.
(3) Wem sind sie wie wichtig? Durch die Bewertung bzgl. Eigentumsrechten, Vertraulichkeit, Verfügbarkeit, Integrität und Compliance-Auflagen wird das Informationen-Register angereichert.

Neben der trivialen Erkenntnis, dass das BI als Management Instrument für Controlling und Analyse sowie für Planung genutzt wird und somit die wesentlichen Schutzziele die Integrität der Informationen und Vertraulichkeit der Geschäftsgeheimnisse betreffen, überrascht die BIA häufig mit der Erkenntnis, dass das BI deutlich darüber hinaus genutzt wird und entsprechend zu schützen ist:

Die Schutzziele der ISO27001

(1) Die **Verfügbarkeit** garantiert berechtigten Nutzern den Zugriff auf Informationen und Daten tragende Systeme zum jeweils erforderlichen Zeitpunkt

(2) Die **Vertraulichkeit** stellt sicher, dass bestimmte Informationen nur durch berechtigte Personen, Instanzen oder Prozesse eingesehen werden können:
- Selbstschutz: geschäftskritische Informationen und Know How
- gesetzlicher Schutz: personenbezogene Daten von Mitarbeitern, Kunden und Partnern (Basis BDSG, ggf Branchengesetze wie TKG)

(3) Die **Integrität** sorgt für vollständige und unversehrte Daten (korrekt, unveränderbar oder Veränderung unleugbar), Daten tragende Systeme und Daten verarbeitende Prozesse.

(4) Die **Compliance** mit allen auf die vorgehaltenen Informationen anwendbaren gesetzlichen Anforderungen. Beispiele:
- Speicherung und Nutzung: Müssen vs. Dürfen (legitimierende Zwecke) vs. Vermeiden
- Aufbewahrungsfristen: Mindestdauer vs. Höchstdauer
- Informationspflichten an Behörden

- Konsolidierung von Bilanzen: Zusätzliche Anforderungen sind hier zeitgerechte Verfügbarkeit (Fast-Close-Prozess und ggf. Pönale der Börsenaufsicht) und Compliance bzgl. HGB, AktG, AO etc.
- Regelberichte an Behörden: Auch hier stehen zeitgerechte Verfügbarkeit integrer Informationen und ggf. Vertraulichkeit und Datenschutz im Vordergrund.
- steuernde Folgesysteme (zum Beispiel Umsteuerung von Logistikflüssen): Hier steht insbesondere die zeitgerechte untertägige Verfügbarkeit ggf. near-realtime im Fokus.

Als Shared Service für viele BI-Kunden mit z.T. sehr unterschiedlichen Anforderungen hat das BI eine herausragende Stellung im Unternehmen – mit der Konsequenz, dass jeweils die stärkste Anforderung der verschiedenen BI-Kunden bestimmend ist für die Auslegung des BI.

Wer oder was bedroht den Hort?

Ausgangspunkt für die Bedrohungslage sind die Faktoren der Umfeldsituation wie:

(1) Kreis der Nutzer: Gibt es jenseits der internen Fachanwender einen erweiterten Personenkreis? Wie sieht die geographische Verteilung und Anbindung der Anwender aus?
(2) Gestaltung und Betrieb des BI: Die Bandbreite reicht von Inhouse-Lösung mit eigenem Betrieb bis SaaS.
(3) Unternehmensspezifika: eigener Erfolg, Aggressivität der Mitbewerber, politische Situation

Die systematische Analyse der Risiken soll dabei über die Betrachtung möglicher Katastrophen hinaus insbesondere Vorsatz durch Spionage, Gegner des Geschäftsmodells und Innentäter sowie Nachlässigkeit durch organisatorische oder persönliche Defizite und Unwissenheit durch Mängel im Rollout von Regeln und Prozessen aber auch natürliche Erosion von Wissen um Risiken, Regeln und Prozesse zu berücksichtigen.

In Abhängigkeit der im BI vorgehaltenen Informationen und der Umfeldsituation sind die Höhe des Schutzbedarfs (Control Objectives) festzulegen, die entsprechenden Maßnahmen (Controls) abzuleiten und in einem BI-Sicherheitskonzept zusammenzufassen.

Das BI-Sicherheitskonzept – Erfolgsfaktoren für den Hort

Ein verbreiteter Irrtum ist, es sei hinreichend, das BI in die Hände eines ISO27001-zertifizierten Dienstleisters zu geben. Er kennt weder die Schutzwürdigkeit der anvertrauten Daten noch die damit verbundenen konkreten Risiken und notwendigen Maßnahmen.

Unter allen Schutzzielen hat die Integrität der Informationen eine herausragende Rolle, denn sie ist die Ware des Hortes BI. Ein Mangel bei Vollständigkeit und Korrektheit der Informationen führt unweigerlich zu signifikanten unternehmerischen Fehleinschätzungen, weil z.B. Analysen von Zielabweichungen und deren Ursachen nicht verlässlich sind und auf Analysen basierende Entscheidungen massive Schäden bei der Umsetzung verursachen können. Daher hat Integrität immer Vorrang vor zeitlichen Aspekten wie Time-to-Market von neuen Modellen!

Aus diesen Punkten können die wesentliche Erfolgsfaktoren für die Umsetzung des BI-Sicherheitskonzepts abgeleitet werden: (1) klare Governance, (2) definierte Prozesse, (3) strukturiertes Einbinden von Stakeholdern.

Governance

Das BI-Competence Center (BI-CC) ist mit zentralen Verantwortungen aufzusetzen, um dem Zerfall der IS insbesondere der Integrität unter dem Druck diverser Interessen von BI-Kunden zu widerstehen. Dies beinhaltet die wesentlichen Rollen

- Gesamtverantwortung gegenüber Geschäftsführung und BI-Kunden
- BI-Information Architecture: Aufbau und Pflege der semantischen Informations-Modelle insbes. Glossar mit den offiziellen Definitionen der KPIs
- BI-Services Management mit der fachlichen Verantwortung für Request und Change Management
- BI-Service Delivery Management: Steuerung der eigenen Wertschöpfungsanteile und der Dienstleister
- BI-Risk & Compliance Management, zu dem auch der Datenschutz gehört

Auch wenn das BI-CC mit seiner großen Nähe zu den Fachbereichen eine gewisse Unabhängigkeit von der stabilen IT der Wertschöpfungskette sucht und Flexibilität sowie Time-to-Market Aspekte in den Fordergrund stellt, das BI ist stets in den gesamten Unternehmenskontext eingebettet; es darf daher keine Regelungs- oder Prozesslücke zwischen BI-CC und anderen Organisationseinheiten insbesondere der IT entstehen.

Dabei sollte Bewährtes unbedingt genutzt oder für BI geeignet ergänzt werden. Hier sind insbesondere Richtlinien, Prozesse, Shared Services aus folgenden Bereichen zu nennen: Corporate Risk & Compliance Management, Corporate Information Security Management, vorhandene Dokumentenklassifikation (intern oder behördlich vorgeschrieben).

Prozesse des BI-CC

Damit das BI-CC, die IT und Dienstleister zielorientiert und abgestimmt handeln, sind der Aufbau der Betriebsorganisation und entsprechende Prozesse zu definieren. Hier kann ITIL V3 als Best Practice dienen.

Aufgrund der hohen Anforderungen an die Flexibilität der von BI bereitzustellenden Services benötigen die folgenden Prozesse einen hohen Reifegrad:

- Betrieb: Das tägliche Monitoring beinhaltet auch die Aspekte Security und Data Quality.
- Change Management: Um sicher und schnell von einem stabilen und zulässigen Zustand in den nächsten zugelangen, sind Impact-Analysen mit Risiko- und Compliance-Aspekten, das systematische Fortschreiben der Informationsmodelle und KPI-Definitionen, und die Dokumentation des neuen Zustands inklusive der Compliance als integraler Bestandteil zu implementieren.
- Restart & Recovery Management: Damit im Ernstfall das BI nicht nur zeitnah und mit geschützter Vertraulichkeit sondern auch mit einem integeren Datenbestand wieder anlaufen kann, sind diese Prozeduren regelmäßig zu üben.

Stakeholder
Das regelmäßige und strukturierte Einbinden von unternehmensinternen Organisationen ist der wesentliche Faktor für den nachhaltigen Erfolg und die Sicherheit des BI und sollte in der Governance verankert werden. So sind die BI-Kunden nicht nur als Anforderer zu sehen, sondern als maßgebliche Unterstützer in den Rollen Master Data Stewards und Data Quality Stewards. Dem Bereich Finance & Controlling steht die führende Rolle bei der Bewertung von Mengengerüsten im Zusammenhang mit handels- bzw. steuerrechtlicher Compliance zu. Natürlich dürfen die Bereiche IT und IT-Dienstleister und Corporate Risk & Compliance nicht vergessen werden.

Bei Einführung oder Umbau von BI und BI-CC stehen in der Regel der Branchenverband, BITKOM (insbes. für BI „Arbeitskreis Big Data" und div. Arbeitskreise für Sicherheit) sowie die itSMF für Service Management und Sicherheit mit Rat und Tat zur Seite. Darüber hinaus empfiehlt sich für eine differenzierte Beratung oder Abstimmung der persönliche Kontakt mit Behörden wie für Datenschutz der Landesbeauftragte oder Bundesbeauftragte, für IT-Sicherheit das BSI und für Wirtschaftskriminalität je nach Sachlage LKA, BKA oder Verfassungsschutz.

Fazit
Ein BI ist keine Ware von der Stange – der Schutzbedarf des BI und dessen Umsetzung sind in hohem Maße unternehmensindividuell.

Typische Fehler beim Aufbau und Betrieb eines sicheren BI sind vermeidbar. Wesentlich dafür ist, rechtzeitig Vertrauen in die Expertise und Zuverlässigkeit von Partnern aufzubauen. Berater, die mit Methodik und Erfahrung in Bezug auf IS und Compliance einerseits und Knowhow in BI andererseits aufwarten, müssen Hand in Hand mit einem zuverlässigen Partner für Implementierung und Betrieb arbeiten können. Mit den für IS wichtigen Schlüsselfähigkeiten in den Bereichen BI-Architektur, BI-Information Management, Data Quality Management sowie ITIL-basiertem BI-Betrieb und Change Management zur Wahrung der Informations-Integrität ist ORAYLIS der BI-Competence Partner, der durch Augenmaß und Zielorientierung herausragt.

Die Autoren

Dr. Bodo Glaser ist selbständiger Managementberater mit den Themenschwerpunkten Business Transformation, Business & IT-Effizienz und Risk & Compliance Management

Alexander Thume ist Senior Consultant bei der ORAYLIS GmbH und spezialisiert auf die Technische Projektleitung und Architektur unternehmensweiter Data-Warehouse-Lösungen

ORAYLIS Business Intelligence

ORAYLIS GmbH
Die ORAYLIS GmbH ist führender Anbieter von Business-Intelligence- (BI) und Big-Data-Lösungen. Basis bilden dabei die zukunftsweisenden Technologien von Microsoft und Tableau Software. Umfassende Projekterfahrung sowie entsprechende Branchenexpertise sorgen für eine erfolgreiche und wirtschaftliche Umsetzung. In diesem Kontext führt ein eigens von ORAYLIS entwickeltes Vorgehensmodell aus Best-Practice-Methoden, darauf abgestimmten Werkzeugen sowie neuesten Technologien gezielt und sicher durch die Projekte.

Dank der herausragenden Leistungen im Data-Warehouse-Umfeld wurde das Unternehmen im Jahr 2012 zum „Partner des Jahres" von Microsoft und HP gekürt.

Kompetenzen
- Innovation
- Standards
- Project Management
- Data Analytics
- Data Management
- BI-Operations

Eingesetzte Produkte
- Microsoft SQL Server
- Microsoft SharePoint Server
- Microsoft Office 365
- Microsoft Power BI
- Tableau Software

Referenzen
ORAYLIS ist unter anderem für namhafte Kunden aus den Bereichen Handel, Industrie und Telekommunikation tätig. Hierzu zählen Bayer, Krones, Vodafone, E-Plus, Karstadt, REWE, OBI und Volkswagen.