IT-Verbund endica der Stadtwerke

Essay Managementsystem – IT Security

IT Sicherheit im Umfeld kommunaler Unternehmen, am Beispiel von Stadt- und Gemeindewerken

Vortragsreihe 2014 – VKU Akademie Leipzig 16. Januar 2014
Köln 11. Februar 2014

IT-Verbund endica der Stadtwerke

IT – Security

Vor dem Hintergrund von **E-Government** und die damit verbundene Digitalisierung in der modernen öffentlichen Verwaltung und bei Unternehmen in öffentlicher Hand, ist Datenschutz und Datensicherheit eine noch größere Herausforderung für die verantwortlichen Mitarbeiter geworden. Der immer häufigere Einsatz von web-basierten Anwendungen, web-basierter Kommunikation zwischen Bürger und öffentlicher Verwaltung, die enorm gestiegene digitale Speicherung von persönlichen Daten, Informationen und Dokumenten sowie der zunehmende elektronische Informationsaustausch zwischen Behörden und Dritten, erfordern verbesserte und sorgfältig ausgearbeitete Maßnahmen und Vorkehrungen. Andernfalls kann ein erfolgreicher Datenschutz nicht garantiert werden.

Die aktuellen Fragestellungen im Datenschutz betreffen ebenfalls den Beschäftigtendatenschutz. Personalabteilungen der öffentlichen Behörden und Unternehmen des öffentlichen Rechts sind heutzutage mit verschiedenen Problemen im Umgang mit Arbeitnehmerdaten konfrontiert. Sie bearbeiten nicht nur Daten der bereits eingestellten Mitarbeiter, sondern erheben einen großen Umfang an Daten im Bewerbungs-und Einstellungsverfahren.

Was also ist Datenschutz und Datensicherheit generell und im Besonderen in der öffentlichen Verwaltung

Datenschutz und Datensicherheit haben das Ziel, Daten jeglicher Art in ausreichendem Maß vor Verlust, Manipulation, unberechtigter Kenntnisnahme durch Dritte und anderen Bedrohungen zu schützen.
Datenschutz ist der Schutz (vorrangig BDSG) von personenbezogenen Daten vor Missbrauch, unberechtigter Einsicht oder Verwendung, Änderung oder Verfälschung („Beeinträchtigung des Persönlichkeitsrechts").
Datensicherheit ist die Gesamtheit der organisatorischen und technischen Maßnahmen, die Verlust und Verfälschung sowie unberechtigte Aneignung von Daten verhindern soll.

Allgemeine Entwicklung	
1970	Bürgerrechtsthema - Politisierung des Datenschutzes
Ende der 70-er	Verrechtlichung und Institutionalisierung mit Recht auf informelle Selbstbestimmung, gestärkt durch das Völkszählungsurteil
Mitte der 90-er	Technisierung des Datenschutzes (Privacy-Enhancing-Technologies), Leitlinie: Datenschutz durch Technik
2000	Ökonomisierung des Datenschutzes, Leitlinie: Privacy sells
2006	Datenschutz durch Prozessmanagement

Heute werden Daten in zunehmenden Maße elektronisch gespeichert und übermittelt. Die elektronischen Datenverarbeitung gewinnt so an Bedeutung und die Herausforderungen für IT zur Beherrschung von Komplexität und Risiken wachsen stetig und viele Fragen bei der Erhebung, Verarbeitung, Verteilung und Speicherung von Daten müssen geklärt werden:

- Wie kann man einen sicheren Datenschutz und Beschäftigtendatenschutz gewährleisten?
- Welche Daten und Verfahren sind in erster Linie gefährdet und benötigen besonderen Schutz?
- Welche Probleme können sich im E-Mail Datenverkehr ergeben?
- Wie können öffentliche Verwaltungen und Unternehmen in öffentlicher Hand die richtige Balance zwischen Transparenz und Internet-Präsenz auf der einen Seite und Datenschutz auf der anderen Seite finden?
- Wie können Personalabteilungen gewährleisten, dass sie rechtskonform mit Beschäftigtendaten umgehen?

Die komplexität der Fragestellung sollte allerdings nicht nur aus der reinen Perspektive von rechtlichen Rahmenbedingungen betrachtet werden. Es geht vielmehr darum gerade Datenschutz und Datensicherheit im Gesamtkontext der **Schutzbedürfnisse** insgesamt zu beleuchten. Das gilt insbesondere für kommunale Stadt- und Gemeindewerke, die sich im öffentlichen Wettbewerb auch und insbesondere gegenüber der Privatwirtschaft behaupten müssen und gleichzeitig der kommunalen Verpflichtung zur Sicherstellung der Daseinsvorsorge nachkommen müssen, in dem umfassend regulierten Branchenumfeld.

Die Schutzbedürfnisse von Stadt- und Gemeindewerken sind bestimmt von den Geschäftsfeldern (Sparten) mit deren spezifischen Anforderungen und Risiken, von den klassischen unternehmerischen Aufgabenstellung im wettbewerblichen Umfeld der Energiebranche, der Verpflichtung zur Daseinsvorsorge sowie von gesetzlichen Bestimmung, die einzuhalten sind.

- Gebäude, Betriebsstätten und technische Einrichtungen
- Versorgungs-Infrastruktur (Stromnetze, Gasnetze, Wärmenetze....)
- Informationstechnologie (IT-Komponenten, LAN/WAN, WEB, Applikationen, Datenbanken)
- Betriebsgeheimnisse und betriebswirtschaftliche Informationen
- Mitarbeiterinformationen- und Verträge (Stammdaten, Verträge, Abrechnungen...)
- Kundeninformationen- und Verträge (Stammdaten, Tarife, Verträge, Abrechnungen...)
- Lieferanteninformationen- und Verträge (Beschaffung, Entgelte ...)
- Verbrauchsdaten/Verbrauchsverhalten aller Kunden und Sparten
- Bilanzierungsdaten aller Sparten (MaBis, KoV5 ....)
- Marke, Image und Reputation

Der Schutzbedarf adressiert nicht ausschließlich Datenschutz und Datensicherheit, sondern insbesondere auch Versorgungssicherheit, Krisenprävention (Business Continuity) und Risikovorsorge. Insoweit ein weit umfassenderes Management von Chancen und Risiken im Gesamtkontext von unternehmerischer Führung und interner Kontrolle (IKS), über die gesetzlichen Normen hinaus, zur Bestandssicherung und Stärkung des Unternehmens bzw. Eigenbetriebes.

IT-Verbund endica der Stadtwerke

IT – Security

Neben den allgemeinen Bestimmung und den gewohnten unternehmerischen Herausforderungen hat mit zunehmender **Liberalisierung** die elektronische Verarbeitung, Kommunikation und Speicherung gewöhnlicher Geschäftsdaten sowie sensibler unternehmerischer und vor allem besonders schützenwerter Daten eine neue Dimension fremdbestimmter Regeln geschaffen.

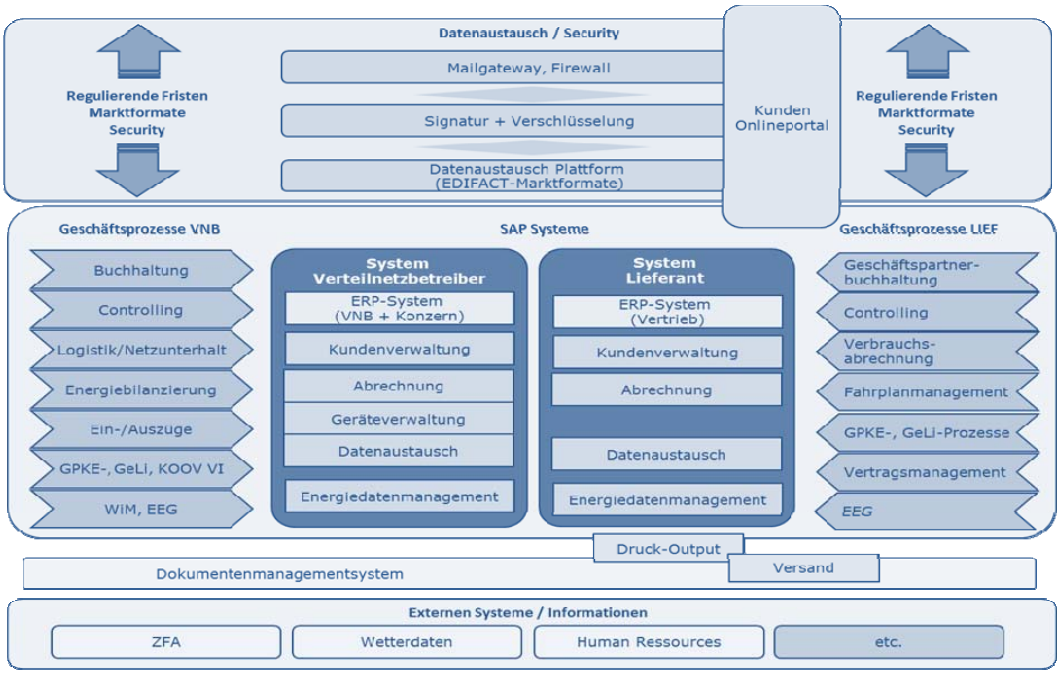
Nicht nur die Entflechtung der sogenannten vertikal integrierten EVU, mit in Folge unabhängiger rechtlicher, operativer, informeller, IT-technischer und buchhalterischer Organisation, sondern vielmehr auch die präzisen Vorgaben zur Kommunikation zwischen den Marktpartnern mit heute mehr als 100 Datenaustauschprozessen, mehr als 685 Zertifikate (Signatur/Verschlüsselung) und über 30 EDIFACT-Formate (UTILMD, MSCONS, INVOIC etc.) mittels e-mail gestütztem Nachrichtenverkehr, über die große Datenwolke WWW, müssen umgesetzt sein und beherrscht werden.

Die Herausforderung an dieser Stelle umfasste daher nicht nur die typischen Stammdaten eines Stadt- oder Gemeindewerkes und das Abrechnungssystem, sondern alle verzahnten SoftwarePakete einschließlich der komplexen Marktkommunikation. Die **praktische Umsetzung** bei en*dica* war bestimmt von Integration und Standardisierung, die neben einer dedizierten Rechtekonzeption (Benutzerkonzept) Konformität in vielen Governance- und Compliance-Fragen gewährleistet:

- SAP Enterprise Ressource Planning
- SAP Abrechnungssystem (IS-U)
- SAP HR (Personalwesen)
- DMS Dokumentenmanagement und Archiv
- Standardisierte Schnittstellen (ZFA, Wetterdaten etc.)
- Integrierte Marktkommunikation

Die Datenqualität (completeness, validity, consistency, timeliness and accuracy), also Vollständigkeit, Gültigkeit, Konsistenz, Aktualität und Genauigkeit bestimmen das Zusammenspiel der Lösungskomponenten. Ansonsten eben der Schutz von Daten und die Sicherheit von Daten, nicht nur in den zentralen Outsourcing-Lösungen, sondern vor allem für die Marktkommunikation von und hin zu den Marktpartnern in den unterschiedlichen Marktrollen und von bzw. hin zu Endkunden.

Das **Systemmodell** und die Architektur der endica-Lösung für Stadt- und Gemeindewerke setzt vorrangig auf Integration und ist als ServiceOrientierteArchitektur, ausgelegt vorrangig entlang der regulierten Prozesse, mit möglichst wenigen Schnittstellen und mit höchstmöglicher Standardisierung als MultiMandantenSystem ausgelegt, jeweils diskreminierungsfrei für die Marktrollen „Verteilnetzbetreiber“ und „Lieferant“!

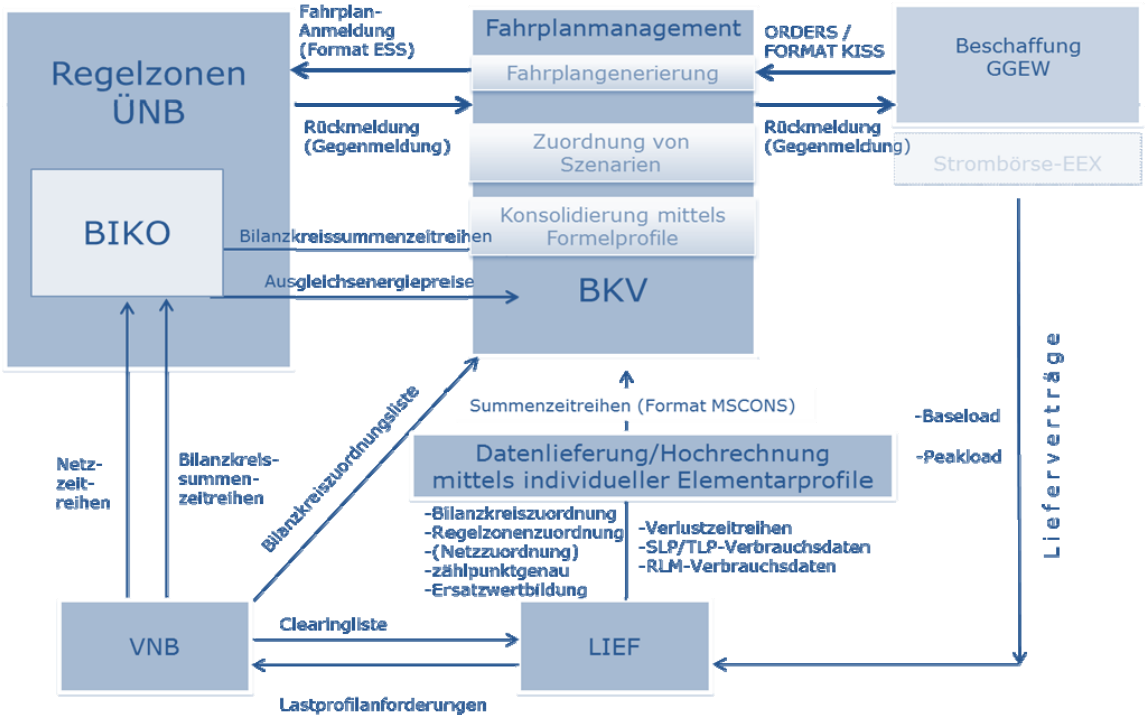


IT-Verbund endica der Stadtwerke

IT – Security

MaBiS Rollenverflechtung

Einen guten Einblick in die Verflechtung(en) von Marktrollen und Marktprozessen zeigen Prozessdokumente zu gesetzlichen Vorschriften und Regelungen, wie z.B. GPKE, Geli, WiM oder wie im Beispiel MaBiS auf.



Marktkommunikation (Zeitsprung Regulierung)

endica hat sich seit Anfang 2012 mit dem Thema Signatur und Verschlüsselung auseinandergesetzt, davon ausgehend, dass die Kommunikationsrichtlinie des BDEW in absehbarer Zeit - wir haben mit 2014 gerechnet - konkrete Maßgaben bzw. Regeln bestimmen wird. Mit zunehmender Regulierung von Datenaustauschprozessen haben insbesondere die klassischen Vorschriften (Gesetze) der Finanzwelt (BMF) an Bedeutung gewonnen und ohne umfassende Signatur bzw. Verschlüsselung ist mittlerweile Marktkommunikation so gut wie nicht mehr möglich.

Der BDEW hat zwar zum 01.10.2012 die Regulierung verschärft, allerdings nur soweit, dass Marktpartner Verschlüsselung/Signatur verlangen können und die Kosten hierfür von den einzelnen Betroffenen selbst getragen werden müssen und die Aufwendungen billigend in Kauf zu nehmen sind. Aber geregelt wurde faktisch nichts. Auch Standards wurde nicht definiert. Mit dem Steuervereinfachungsgesetz 2011 sind gleichwohl nur die Kontrollvorschriften für Leistung/Rechnung nach § 14 UStG, strapaziert worden. Das Thema Signatur und/oder Verschlüsselung allerdings wurde nicht konkretisiert.

IT-Verbund endica der Stadtwerke

IT – Security

Begonnen hat **en*dica*** in 2012 mit der Produktauswahl und der Einrichtung eines Test- und Entwicklungssystems, mit der Maßgabe eine zukunftsfähige skalierbare Lösung zu finden, welche zum 01.01.2014 hätte in Produktion gehen sollen.

Einige Marktpartner haben dann in 2012 begonnen, Nachrichten nur noch signiert und verschlüsselt zu versenden und stillschweigend vorauszusetzen, dass die Marktpartner darauf eingerichtet sind. Das alles ohne Vorankündigung und ohne Vorlaufzeit. Nachrichten konnten plötzlich nicht verarbeitet werden und wir waren gezwungen, weil keiner unserer betroffenen Kunden darauf vorbereitet war, weit vor dem vollständigen Design der Lösung und dem geplanten Announcement, das neue Signatur/Verschlüsselungssystem, produktiv zu setzen!

Mit zunehmender Ausprägung der **Marktkommunikation** und deren architektonischer Ausprägung (Herausforderung - Prozesse/Nachrichten) ergibt sich in der praktischen Umsetzung enormer Abstimmbedarf bzw. die Notwendigkeit, dass sich die Marktteilnehmer im Rahmen der gegebenen Ordnung (rechtlich vorgeschriebener prozessualer Verflechtung) zu bestimmten Regeln der Kommunikation einigen und diese konkret vereinbaren, wie z.B.

- Verschlüsselung
- Signatur
- Datenvorhaltung/Archivierung
- Benutzerverwaltung und Datenschutz

Wenn wir die Schutzbedürfnisse der Marktteilnehmer insgesamt mit reflektieren und von einer geregelten Marktkommunikation zwischen den Marktpartnern ausgehen, ergeben sich entsprechende Ableitungen bezüglich der IT-Architektur.

- Gateway
- Firewall(s)
- Exchange (vs. AS2)
- Viren- und Spamschutz
- Verschlüsselung und Signatur
- Archivierung

Im Geschäftsjahr 2012 haben daher Marktpartner begonnen, sich über die Welt der regulierten Marktliberalisierung hinaus, selbst zu organisieren und ihre Daten individuell zu schützen.
Das führte dazu, dass in der Zwischenzeit 357 von etwa 1.000 Marktpartnern die fortgeschrittene digitale Signatur mit Verschlüsselung einsetzen. Insgesamt sind es Stand heute 685 Zertifikate, die die endica in Ihrem Verbund verwaltet.

Marktkommunikation (Betriebliche Herausforderung)

Durch die anspruchsvolle Architektur, die über mehrere Instanzen, Kontrollpunkte und Gefahrenpunkte zu organisieren ist, ergeben sich naturgemäß in diesem Spannungsbogen viele entscheidende, risikobehaftete Herausforderungen, die es gilt, „unter einen Hut" zu bekommen.

- Durchgängiges Prozessmonitoring, über alle technischen Instanzen hinweg
- Vermeidung von Datenverlusten, Datenredundanzen und Gefährdung der Datenintegrität
- Vermeidung von Schnittstellen bzw. externen Zulieferungen, insbesondere Solcher die nicht architekturkonform und/oder nicht marktkonform sind
- Plausibilisierungs- und Validisierungszwang
- Prozessintegration (um beinahe jeden Preis)

Letztendlich noch professioneller Änderungsdienst, entweder fremdbestimmt für z.B. halbjährliche Formatwechsel oder für selbstbestimmte Veränderungen bei Technologiewandel, Releasewechsel oder Optimierungen.

Marktkommunikation (Lösung)

Marktkommunikation ist ein reguliertes Datenaustauschverfahren mittels formatierter und strukturierter e-mails. Die standardisierte Marktkommunikation, als Datenaustauschverfahren, wird gesteuert über Adressen und Formate, so dass strukturierte Daten und Nachrichten ausgetauscht werden können.

- SAP Exchange Infrastructure (SAP XI / PI), als Integration Broker, zur logischen und inhaltlichen Verarbeitung von formatierten Nachrichten
- Mail-Transportverfahren mit Internetzugang, Gateway, Firewall und Mikrosoft Exchange Server
- Passwortschutz für Anhänge (sofern überhaupt verwendbar oder zweckmäßig – in jedem Falle nur anwendbar außerhalb der regulierten und mit SAP IS-U/SAP EDM verknüpften Marktkommunikations-prozesse)

Zu Beginn waren lediglich 6 Formate für einige wenige Prozesse erforderlich. Heute sind es mehr als 30 Formate, für etwa 100 regulierte Prozesse und es werden künftige noch weit mehr regulierte Prozesse und Formate hinzu kommen.

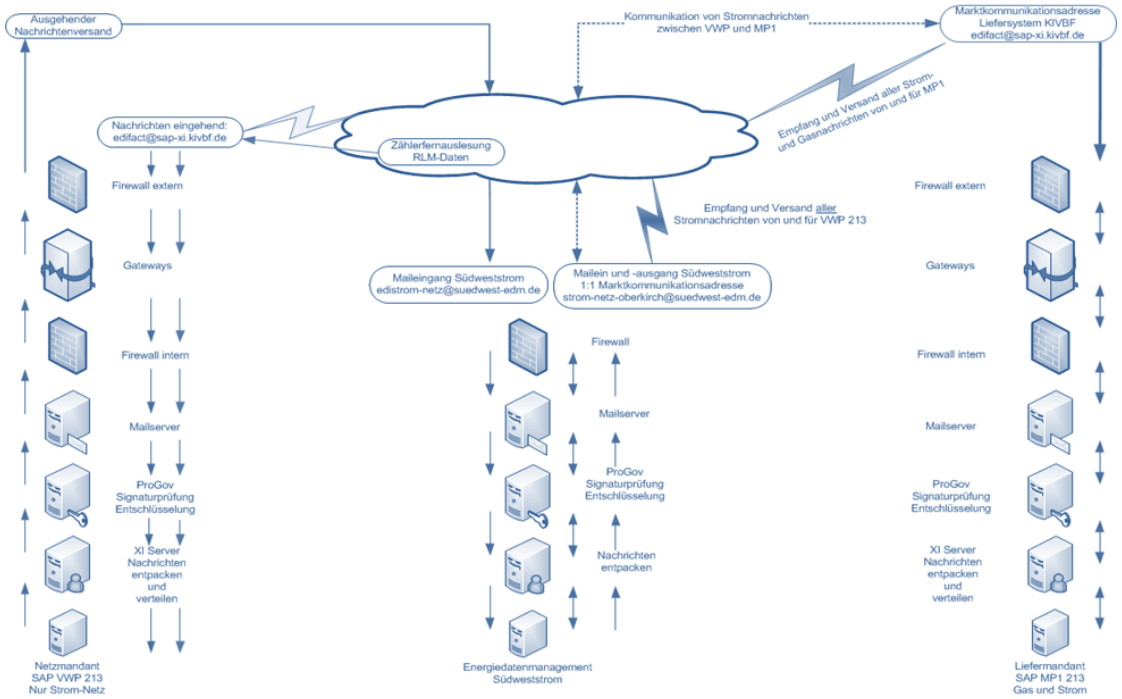
IT-Verbund endica der Stadtwerke

IT – Security

Marktkommunikation (Architektur)

Die Komplexität zeigt klar, dass gerade in der Marktkommunikation fast alle Disziplinen von IT-SEC strapaziert werden:

- Netzwerkzugang (firewall/gateway)
- Viren-/SPAM-schutz
- Schutz vor unberechtigten Angriffen (intrusion dedection)
- Verschlüsselung/Signatur
- Übertragungskontrolle
- Benutzerrechte und Rollenregeln
- Formatkonformität
- Nachweisbarkeit von Originalnachrichten (Archiv)
- Datenintegration (wokflowgestützt in der Verbindung mit SAP-XI (Connector/converter)



Perspektive

Datenschutz und Datensicherheit ist keine losgelöste Geschichte von Einzelkämpfern, namens „Datenschutzbeauftragter", die im steten Diskurs um Wahrnehmung, Priorisierung oder Notwendigkeit Offensichtliches mühsam unter Beweis stellen müssen.

Auch geht es um weit mehr als nur die reine IT-Datenverarbeitung und es geht im Gesamtkontext um weit mehr als eben nur Datenschutz und Datensicherheit alleine, sondern um:

- die Erreichung und Einhaltung unterschiedlicher eigen- oder fremdbestimmter Governance- wie auch Non-Governance Regularien;
- verantwortetes Unternehmertum im Kontext von Unternehmenszielen, Strategien und Risikosteuerung entlang der primären und sekundären Wertschöpfung;
- bewusste Strukturierung des Unternehmens über alle Instanzen hinweg in der Aufbau- wie auch Ablauforganisation, um Rollen und Verantwortlichkeiten sowie Rechte und Pflichten;
- transparente Kontrolle und Steuerung im Gesamtkontext von Risikomanagement, Compliance Management und Internem Kontrollsystem (IKS)

Datenschutz und Datensicherheit muss daher als integrierte Disziplin verstanden werden, mittels dieser sich Kultur, Performance und Professionalität eines Unternehmens über alle Themen hinweg, reflektiert.

Nur im steten Dialog und Schulterschluss aller Betroffenen und Beteiligten ist Datenschutz und Datensicherheit praktisch angewandtes Kulturgut und nicht nur mühevolle Cross-Funktion vorrangig mit Kontrollaufgaben.

Nur wenn Datenschutz und Datensicherheit in alle steuerungs- und führungsrelevanten Fragestellungen mit eingebunden wird, ist das Thema nachhaltig wirksam im Unternehmen zu verankern.

ENDE