SCHUTZ DER KRITISCHEN INFRASTRUKTUREN: EIN STRATEGISCHER GESAMTBLICK

Dr. Peter Kanyion, Risiko Manager @ SYSback AG
Björn Bausch, IT-Forensiker und Datenschützer @ best-practice innovations gmbh
Axel Himmelreich, Sales & Business Development @ SYSback AG

ISD2017, Brühl 28.09.2017

INFORMATIONSMAPPE

Unser Geschenk an Sie!

- Dr. WEB Enterprise Security Suite
  für 2 Monate Gratis Schutz und 40 % Preisvorteil beim Kauf
- Fachzeitschrift ‚ITSMF Magazin Nr. 35' mit Artikel wie IT-Sicherheit 4.0 und Automation Toolauswahl / Automation Roadmap im Gegenwert von 14 €
- SYSback Mobile Card Holder
- Whitepapers zu
  - NETAPP Private Storage as a Service
  - Colocation im sichersten Rechenzentrum
  - Sichere und einfacher Backupdaten-Speicher für Behörden
  - Veeam Cloud Connect Backup-Lösungen
- b-pi und SYSback Unternehmensinfos

Kann nach dem Vortrag bei uns abgeholt werden!

AGENDA

- Begrüßung & Kurze Personenvorstellung
- EU-DSGVO: Sicherstellung der Compliance
- Einführungskonzept ISMS inkl. BSI-Grundschutz und EU-DSGVO
- KRITIS – Unterstützung durch Enterprise Architektur Management
- KRITIS – Unterstützung durch Automation
- SYSback & b-pi Services – Ein Überblick
- Warum b-pi und SYSback?
- Forum Moderation – Fragen und Antworten
- Informationsmappe

EU-DSGVO: SICHERSTELLUNG DER COMPLIANCE ‚TRIGGER FOR COMPLIANCE‘

SCOPE

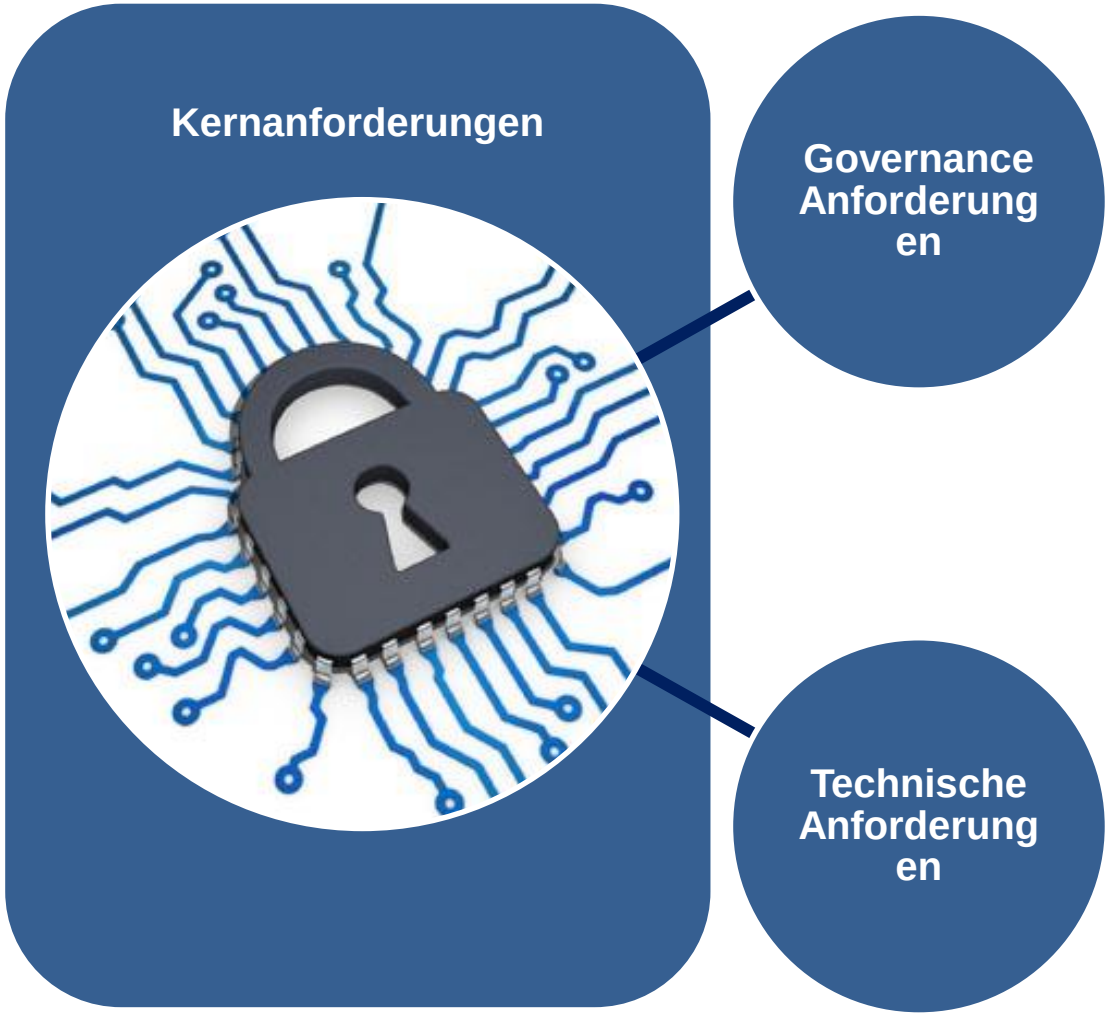
- **25. Mai 2016**
  Inkrafttreten der GS-GVO
- **25. Mai 2018**
  Deadline für Compliance

SANKTIONEN

- **4% bzw. 20 Mio. €**
  Nichteinhalten der Rechte der Betroffenen
- **2% bzw. 10 Mio. €**
  Nicht Einhaltung der spezifizierten Kontrollen

DS-GVO findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen der Union (EU), unabhängig davon, wo die Verarbeitung stattfindet.

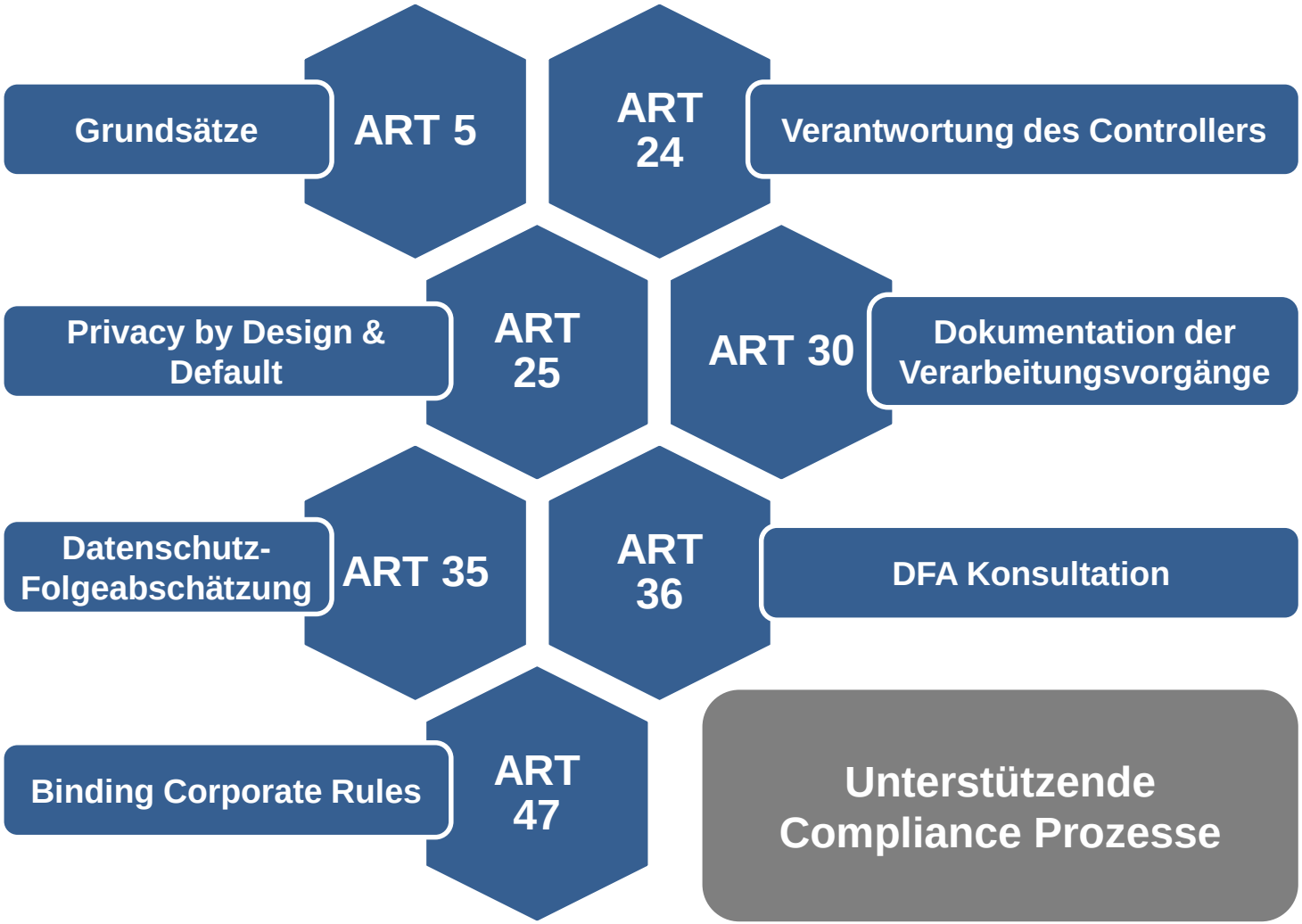
EU-DSGVO: SICHERSTELLUNG DER COMPLIANCE ‚KEY REQUIREMENTS & CAPABILITIES‘



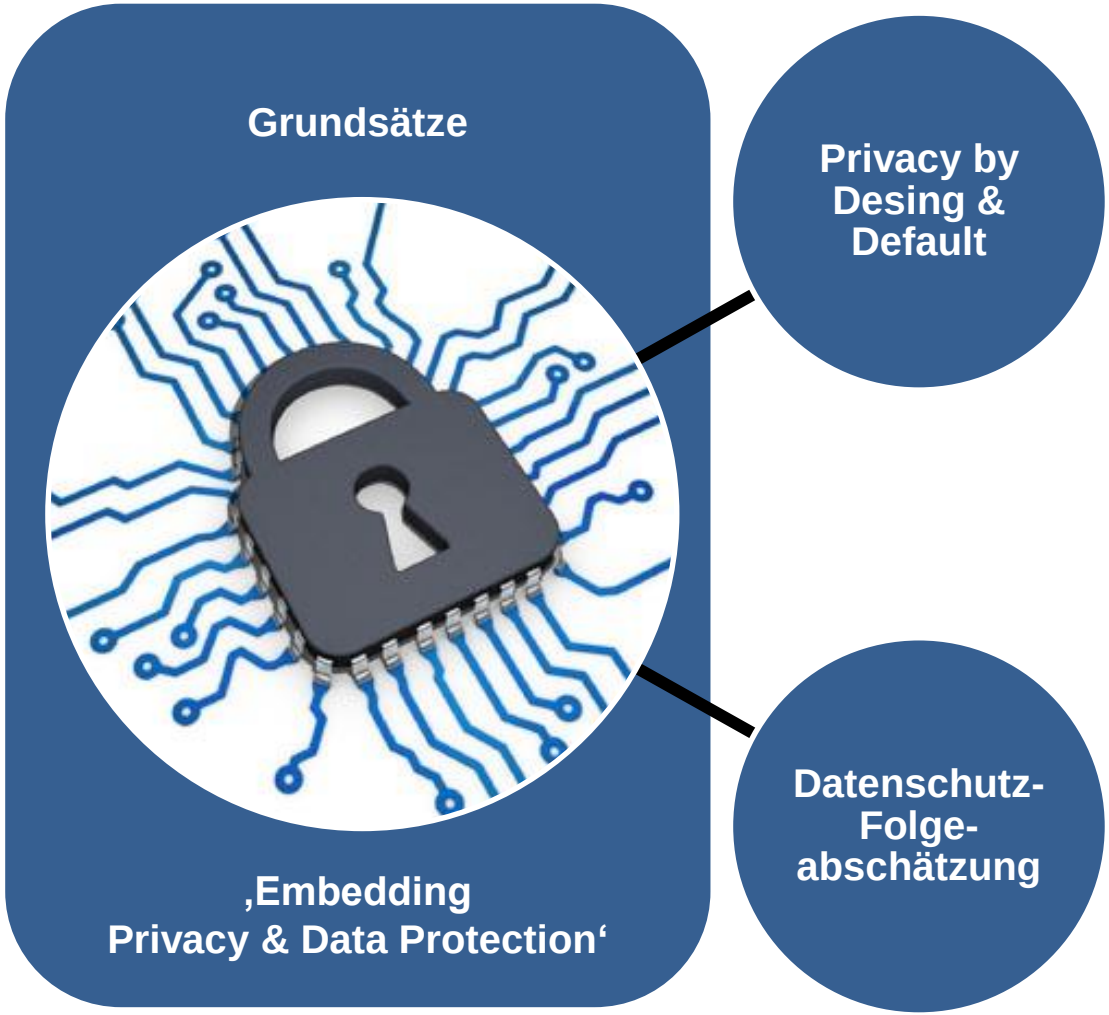
- Bestätigte Einwilligung
- Compliance
- Meldungen von Datenschutzverstößen
- Legitime Verarbeitungszwecke
- Datenschutzbeauftragter

- Sichere Speicherung
- Datenübertragbarkeit
- Richtigkeit der Daten
- Berichtigung/Löschung

EU-DSGVO: SICHERSTELLUNG DER COMPLIANCE ‚PRIVACY MANAGEMENT RULES'



EU-DSGVO: SICHERSTELLUNG DER COMPLIANCE ‚OPERATIONALIZATION OF PRINCIPLES‘



- **Institutionalisierung des Datenschutzmanagement**
- **Integrative Anwendung technischer Schutzmaßnahmen**

- **Bewertung der Datenschutzauswirkungen**
- **Angemessene Abschätzung der Risiken**

EU-DSGVO: SICHERSTELLUNG DER COMPLIANCE ‚COMPLIANCE APPROACH‘

- Anwendbarkeit festgelegt
- Kontrollen des Informationssicherheitsrahmenwerkes evaluieren
- GAP-Analysen Durchführen

FAKTEN ZUR EU-DSGVO (1/5)

Ausgangspunkt:

- EU-Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
- 10.2003 neue Datenschutzverordnung vom Europäischen Parlament auf den Weg gebracht

  → am 12.03.2014 verabschiedet
- Änderungen der geplanten EU-Verordnung (Fassung des EU-Parlaments) gegenüber der Richtlinie aus 1995 nach dem derzeitigen Stand:

FAKTEN ZUR EU-DSGVO (2/5)

Änderungen der geplanten EU-Verordnung gegenüber der Richtlinie aus 1995 nach dem Stand der Veröffentlichung der EU-DSGVO im EU-Amtsblatt, 14.4.2016 :

Mehr Datenschutzbeauftragte:

- Erstmalig europaweite geltende Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten
- Die EU-DSGVO erfordert zukünftig die Benennung eines Datenschutzbeauftragten und die Mitteilung an die Aufsichtsbehörden, sofern eine „Benennungspflicht“ besteht

Ausdrückliche Einwilligung zur Datenerarbeitung:

- Verarbeitung und Weitergabe persönlicher Daten ohne Einwilligung des Nutzers nur noch beschränkt möglich
- Nutzer explizit um Einverständniserklärung bitten
- Einwilligung nicht im Kleingedruckten, sondern gut sichtbar (standardisierte, einfach zu erkennende Symbole / Icons)
- Keine Erstellung von Nutzer-Profilen, wenn Nutzer dies verbietet
- Für Daten von unter 16-jährigen Einwilligung der Eltern erforderlich

FAKTEN ZUR EU-DSGVO (3/5)

Datenweitergabe nur nach EU-Recht:

- Datenweitergabe an Drittstaaten wie die USA zukünftig ausschließlich auf Grundlage von EU-Recht möglich

Gebot der Datensparsamkeit:

- Bei der Abfrage von Daten so datensparsam wie möglich
- Bei Benutzereinrichtung nur die datenschutzfreundlichen Voreinstellungen verwenden
- Dienste auch unter Pseudonym oder anonym nutzbar

Drastische erhöhte Sanktionen:

- Je nach Delikt unterschiedlich
  - 10 Millionen oder 2% des weltweiten Umsatzes
  - 20 Millionen oder 4% des weltweiten Umsatzes bei schweren Vergehen

FAKTEN ZUR EU-DSGVO (4/5)

Recht auf Löschen der Daten:

- Will der Nutzer seine Daten löschen lassen, dann braucht er sich nur an den Anbieter zu wenden, der die Informationen zuerst aufgenommen und eventuell weitergegeben hat

  → Dieser muss sich dann um die Löschung kümmern

Einheitliches Recht:

- Einfacheres Vorgehen eines Nutzers gegen Anbieter, wenn diese ihren Sitz nicht in Deutschland haben (bisher galt Recht des jeweiligen Landes)
- Sogar weltweit europäisches Recht, wenn Daten von EU-Bürgern betroffen sind

Konzernprivileg:

- Austausch von Daten innerhalb eines Konzerns/Unternehmensgruppe vereinfacht
- Benennung eines Konzern-Datenschutzbeauftragten wird ausdrücklich vorgesehen

FAKTEN ZUR EU-DSGVO (5/5)

Inkrafttreten:

- 12.03.2014 passierte die EU-Datenschutzverordnung mit den Änderungen des Berichterstatters Jan-Phillipp Albrecht die erste Lesung des EU-Parlaments
  (621 dafür, 10 dagegen, 22 Enthaltungen)
- 15.06.2015 erfolgte die Einigung der EU-Justizminister im Ministerrat
- Anschließend Beginn des „Trilogs“ – endgültige Abstimmung zwischen Kommission, EU-Parlament und Ministerrat
- 25.05.2016 Verabschiedung EU-Datenschutzgrundverordnung
- Bis 25.05.2018 endgültiges Inkrafttreten

IT-SICHERHEITSKONZEPT GEMÄSS BSI (1/2)

Objektbezogen

- Systemtechnisches Umfeld ändern
- Neuorganisation des Büros
- Einsichtnahme Dritter verhindern
- Umsetzen der Arbeitsplatzrichtlinie

Organisatorisch

- Datenträgerverwaltung organisieren
- Wartung und Reparaturen
- Softwareeinsatz (nur freigegebene SW verwenden)
- Regelmäßige Kontrolle des Softwarebestands mit Aktualisierungen
- verwenden von (sicheren) Passwörtern
- PC-Richtlinien
- PC-/Störungs-Checkheft
- Entsorgung Betriebsmittel

IT-SICHERHEITSKONZEPT GEMÄSS BSI (2/2)

Personell

- Schulung, Unterweisung
- schriftliche Sicherheitshinweise, Merkblätter

Hardware/ Software

- Zugangskontrolle
- Passwortschutz (BIOS)
- Virenschutz
- USB-Gerätesetzen

Notfallversorgung

- Backup, -verfahren, Restore (Tests auf Funktion!)
- Aufbewahrung Backup
- Medien und andere Datenträger - Notfalldatenträger

IT-SICHERHEITSGESETZ

- Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
- 25.07.2015 in Kraft getreten
- Das Ziel ist es, die Versorgung mit Dienstleistungen Kritischer Infrastrukturen (KRITIS) in Deutschland aufrechtzuerhalten!!!

IT-SICHERHEITSGESETZ: KERNAUSSAGEN

Meldepflicht von erheblichen IT-Sicherheitsvorfällen

- An das BSI

Pflicht zur Einhaltung von IT-Sicherheitsstandards

- Stand der Technik

Betrachtung versorgungskritischer Abteilungen/Einheiten

- Energie → Netzleitstelle

Einhaltung anderer Gesetze (Spezifizierung)

- BNetzA → IT-Sicherheitskatalog

Das Gesetz adressiert:

- Betreiber von Webangeboten (z.B.: Online-Shop-Betreiber)
- Telekommunikationsunternehmen
- KRITIS-Betreiber

IT-SICHERHEITSGESETZ: WICHTIGE FRAGEN

- Wer ist Betreiber einer Kritischen Infrastruktur?
- Wird das Gesetz angepasst?
- Was bedeutet Stand der Technik?
- Schwierigkeiten mit Schwellwerten?
- Wo hört der Verbund auf?

- Schwellwerte je nach Sektor
  → 500.000 versorgte Personen (Energie)
- Spezifiziert wird das Gesetz durch weitere Rechtsverordnungen
- Standards (DIN, ISO usw.)
- Versorger nutzen/mieten Infrastruktur von anderen Versorgern (z.B. Telekom, 1&1)
  → Zusatzproduktionen können den Schwellwert unnötig in die Höhe treiben
- Betroffen sind all diejenigen IT-Systeme,

IT-SICHERHEITSGESETZ: BESONDERHEITEN (1/2)

KRITIS

- Schaffung Sicherheitsmaßnahmen zum Stand der Technik
- Evaluation dieser Maßnahmen alle 4 Jahre (Zertifizierung)

Meldepflicht

- Gilt erst ab der Veröffentlichung der jeweiligen Rechtsverordnung
- Es wird an das BSI gemeldet

Verstöße / Strafen

- Nichteinhaltung der Pflichten aus dem IT-Sicherheitsgesetz
- Bußgelder bis zu 50.000€

Umsetzungen

- Pflicht zur Einhaltung galt ab sofort
- Umsetzungsfrist von 2 Jahren

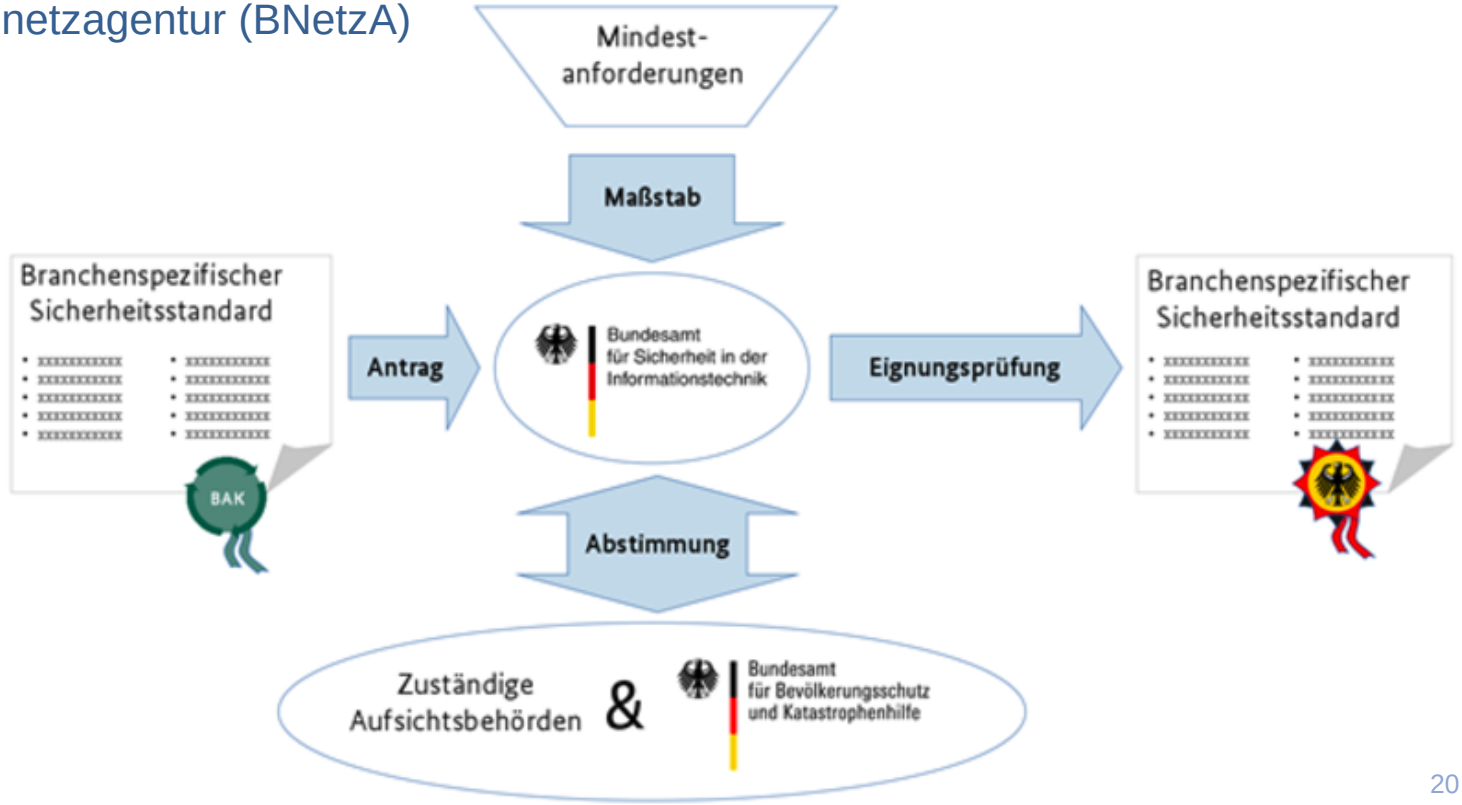
IT-SICHERHEITSGESETZ: BESONDERHEITEN (2/2)

Rechtsverordnungen

- Spezifiziert die KRITIS-Unternehmen

Zwang zum Einhalt der Branchenspezifischen Standards

- B3S (DVGW – Deutscher Verein des Gas- und Wasserfaches e.V.)
- Bundesnetzagentur (BNetzA)



INTEGRIERTES MANAGEMENT SYSTEM: INTEGRATION ISMS UND DSMS (1/2)

Vorteile:

- Managen von einem einzigen System
- Integration aus ISO 27001 / BSI-Grundschutz /VdS 3437 / EU-DSGVO
- Keine doppelte Erfassung von Daten
- Keine redundante Datenhaltung
- Beratung aus einer Hand
- Expertenteam bestehend aus ISB und DSB arbeiten eng zusammen
- Ressourcen werden einmalig gebunden
- Manpower muss nur für ein Projekt gestellt werden
- Budgeteinsparung

INTEGRIERTES MANAGEMENT SYSTEM: INTEGRATION ISMS UND DSMS (2/2)

Information Security Management System (ISMS)

- Erfassung der schützenswerten Assets
- Aufzeigen von Sicherheitsmechanismen
- Erklärung der Sicherheitsmechanismen durch eine geeignete Risikobetrachtung
- Sicherheitsvorfälle: analysieren, reagieren, melden
- Personalsicherheit
- Audits

Data Protection Management System (DSMS)

- Erfassung der Verfahren/Verarbeitungstätigkeiten
- TOM (technische und organisatorische Maßnahmen)
- Erklärung der Sicherheitsmechanismen durch eine geeignete Risikobetrachtung
- Meldung von Vorfällen an die DS-Behörde
- Durchführung von Mitarbeiterschulungen
- Audits

KRITIS – ENTERPRISE ARCHITEKTUR MANAGEMENT

best-practice innovations b-pi SYS back

ARCHITECTURE IS MANAGED

ARCHITECTURE IS NOT MANAGED

“Architecture” Definition:

The Art to Make and Provide, virtually everything, in a Human Dimension.

- **Understandable**
- **Integrable**
- **Usable**

KRITIS – ENTERPRISE ARCHITEKTUR MANAGEMENT

best-practice innovations b-pi

WHAT HAPPENS IF ARCHITECTURE IS NOT MANAGED?

http://www.WinchesterMysteryHouse.com

Key facts about construction

- 38 years building time
- $5.5 million costs ($165 million at today's values)
- 147 craftsmen, 0 architects
- No architectural drawings, no architecture planning

Long-term consequences of lack of planning

- 5 doors lead straight into a wall
- 13 abandoned staircases
- 24 roof windows in corridors

KRITIS – ENTERPRISE ARCHITEKTUR MANAGEMENT

best-practice innovations b-pi SYS back

WHAT HAPPENS IF ARCHITECTURE IS NOT MANAGED?

http://www.WinchesterMysteryHouse.com

Hier & Heute

- **Das Winchester Mystery House ist eine Attraktion!**
- **Aktuelle Architektur Projekte in Deutschland? BER ! ? Vs. Negative Presse …**
- **Wie sieht das in der IT aus?**

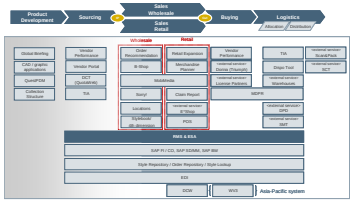
KRITIS – ENTERPRISE ARCHITEKTUR MANAGEMENT

best-practice innovations b-pi SYS back

Urban planning

- Vision of the City
- City Administration, Health, Security …
- Roads, Bridges, Shop, School, Hospital …
- Industrial-/Residential Zone, Nature Park …
- General Infrastructure (electricity, water …)

Enterprise Architecture Management



- Strategy
- Business Processes
- Information, Data, Services
- Applications, IT-Systems
- Infrastructure

Common features

- Complex structure of autonomous systems and their dependencies
- Heterogeneous structures
- Built and financed by many different parties
- Growing continuously
- Long-term perspective for change and investment management

KRITIS – HOLISTISCHE AUTOMATION

VERSION 9.1

Prozess/Methodenwissen, ITIL und Business Prozesse

Technik-, Systemintegrator- und Betriebswissen

Holistische Automation

Automation	**Künstliche Intelligenz / Artificial Intellicence & Holistische Datacenter- und IT-Prozess Automation (RPA):** Reifegrad Analyse, Automation Roadmap, TicketAnalyzer, arago HIRO, Flowster, IPsoft IPcenter, HPE OO, SA, NA, DMA
ITSM*plus*	**ITSM:** HPE Asset Manager, Service Manager, UCMDB, Universal Discovery, Connect-It; PMCS helpLine ITSM; ServiceNow **/ Performance & Capacity Management:** TeamQuest Vityl Monitor, Vityl Advisor, Vityl Dashboard **/ Lizenzmanagement:** Brainware Spider, Vertragsberatung, Technische Beratung, Audit Unterstützung, Metriken, Software Asset Management
EAS	**Enterprise Architektur Services:** Beratung & Konfiguration zum Aufbau von Enterprise Architekturen, OnPrem, Private / Public / Hybrid Cloud Umgebungen, OpenStack, Prozessen und Dokumentation, IT Financial Management mit CODI & SIMCALC
Managed Services	**Betrieb:** 5x9 / 7x24 Service Desk, UHD, Windows Server & Clients, Active Directory, Office365, MS Exchange, Lync, Sharepoint, MS SQL, IIS, Windows Client Applikationen, Virus Scanner, Linux, Apache, MySQL, AS400/iSeries, iOS, Android, Monitoring, Backup/Restore, Rollouts, CapaSystems PerformanceGuard, i-doit, Cloud Backup, AVG Managed Workplace; Betrieb von Automationslösungen
SAP	Alle **SAP Services** für R/3 und alle Nachfolgesystemversionen, NetWeaver und S/4 HANA. SAP Basis Betrieb und Spezialisten für alle SAP Module Umfassende Beratung für SAP Hard- und Software
SDM/PM	**Service Delivery Management & Projekt Management** insb. in Outsourcing Situationen: Bereitstellung erfahrener Projekt Manager, Transition Manager, Service Delivery Manager, Incident-, Change-, Problem- und Config Manager

Nutanix, Rubrik, DARZ, LeaseWeb, IoT, ServiceNow

IBM, HDS, NetApp, EMC, HPE, vmware, Microsoft, SUSE

Handelsware: Hard- und Software

B-PI MISSION UND LEISTUNGEN:
B-PI CONSULTING

best-
practice
innovations

b-pi

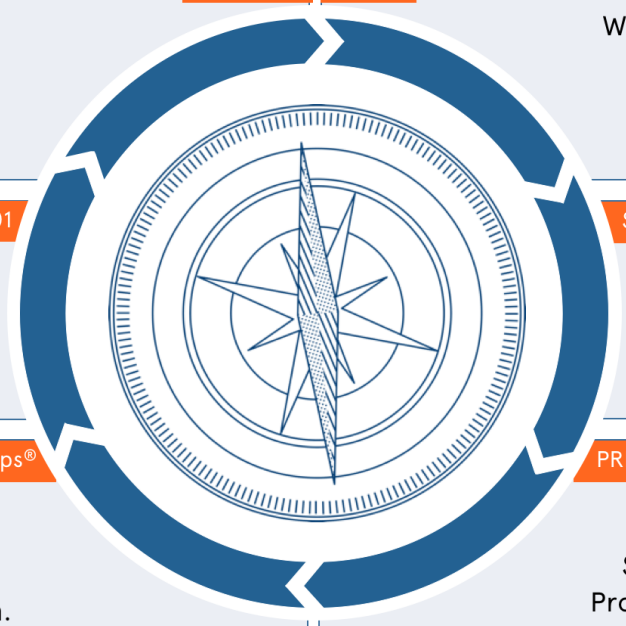
SYS back

Governance, Risk, Compliance (GRC)
Wir helfen Ihnen, regulatorische Anforderungen einzuhalten, Risiken zu mitigieren und Ihre Organisationsstrukturen an den Unternehmenszielen auszurichten.

COBIT5®

ITIL®

Architecture & Service Management (ASM)
Wir unterstützen Sie dabei, Ihre IT-Services zu definieren, deren Reifegrad zu erhöhen und Ihre Architekturlandschaft zu definieren und weiterzuentwickeln.



ISO27001

Security & Data Protection (SDP)
Wir unterstützen Sie beim Management der Informationssicherheit und des Datenschutzes Ihres Unternehmens und beim Aufbau wichtiger CISO-Funktionen.

SGF®

Sourcing & Vendor Management (SVM)
Wir legen gemeinsam mit Ihnen Ihre Sourcing-Strategie fest, identifizieren die geeigneten Vendoren und managen die Leistungserbringung und die Verträge.

DevOps®

Business Process Digitalisation (BPD)
Wir helfen Ihnen, Ihre Prozesse zu digitalisieren, digitale Geschäftsmodelle zu entwickeln und Automatisierung als Kompetenz in der Organisation zu verankern.

PRINCE2®

Project/Programme/Portfolio Management & Support (P^3MS)
Wir unterstützen Sie bei der Planung, Steuerung und Umsetzung von Projekten und Programmen aller Komplexitätsstufen, inklusive qualifiziertem Projektsupport.

SYNERGIEN

- Jahrelange Consultingerfahrung mit agiler Arbeitsweise
- Trainingskurse ISO 27001
- Trainingskurse zum Datenschutzbeauftragten
- Expertise im Bereich ISMS und IT-Grundschutz durch Tochterfirma b-pi sec

- IT-Gesamtdienstleister
- EAS & Technologien zur Umsetzung der Lösungsansätze
- Eigenes Kompetenzcenter für „Holistische Automation“
- Einziger „Multi Vendor Automation Provider“ im Markt

Verzahnte Consultingerfahrungen und Technologielösungen, Trainings & Schulungen:

„Kundenbetreuung von A bis Z“

INFORMATIONSMAPPE

Unser Geschenk an Sie!

- Dr. WEB Enterprise Security Suite
  für 2 Monate Gratis Schutz und 40 % Preisvorteil beim Kauf
- Fachzeitschrift ‚ITSMF Magazin Nr. 35' mit Artikel wie IT-Sicherheit 4.0 und Automation Toolauswahl / Automation Roadmap im Gegenwert von 14 €
- SYSback ‚Mobile Card Holder'
- Whitepapers zu
  - NETAPP Private Storage as a Service
  - Colocation im sichersten Rechenzentrum
  - Sichere und einfacher Backupdaten-Speicher für Behörden
  - Veeam Cloud Connect Backup-Lösungen
- b-pi und SYSback Unternehmensinfos

Kann nach dem Vortrag bei uns abgeholt werden!

VIELEN DANK FÜR DIE AUFMERKSAMKEIT

WIR WÜNSCHEN
INTERESSANTE GESPRÄCHE,
KONSTRUKTIVEN AUSTAUSCH
UND EINE SICHERE HEIMFAHRT

PETER, BJÖRN & AXEL

Dr. Peter Kanyion, Risiko Manager @ SYSback AG
Björn Bausch, IT-Forensiker und Datenschützer @ best-practice innovations gmbh
Axel Himmelreich, Sales & Business Development @ SYSback AG
