



www.dvz-mv.de



Bericht über das ISO 27001/BSI-GS Zertifizierungsprojekt

Jan-Peter Schulz

Senior Security Consultant

Projektleiter RZ-Zertifizierung ISO27001/IT-Grundschutz





- Die DVZ M-V GmbH hat sich zu einer Zertifizierung für das Rechenzentrum nach dem Standard:

ISO 27001 auf der Basis von IT-Grundschutz entschlossen.

Dieser Standard ist vom Bundesamt für Sicherheit in der Informationstechnik (BSI) erarbeitet worden - das Zertifikat wird auch vom BSI selbst vergeben.



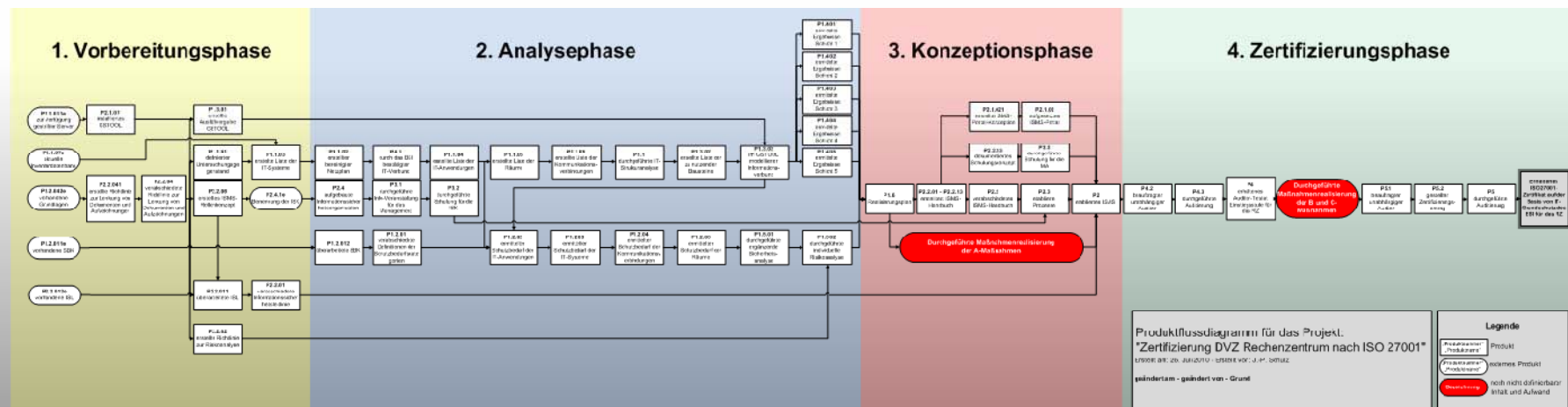


- Erstellung und Verwaltung von ca. 60 Verfahrenssicherheitskonzepten für Kunden seit 2004 auf der zentralen GSTOOL-Installation
- diese beinhalten sowohl zentrale als auch dezentrale Kundenkomponenten
- **Ziel:**
Aufbau und Betrieb eines eigenen, zentralen, zertifizierbaren Informationssicherheitsmanagementsystem (ISMS)
- **Gründe:**
 - Effizienzsteigerung und Verhinderung von Sicherheitsvorfällen
 - Standardisierung und kontinuierliche Verbesserung des ISMS
 - Nachweis des Informationssicherheitsniveaus gegenüber Kunden und Dritten
 - Aufrechterhaltung der bisherigen und Ausbau der Kundenzufriedenheit



Daten und Fakten ...

- Projektdauer: April 2010 – September 2012
- Projektorganisation nach Prince2
- Ein Vollzeit-Projektmanager über die gesamte Projektlaufzeit
- Nutzung des aktuellen GSTOOLS (4.7) vom BSI
- Schaffung einer Vollzeit-Stelle „Informationssicherheitsmanager“





Abgrenzung des Informationsverbunds ...

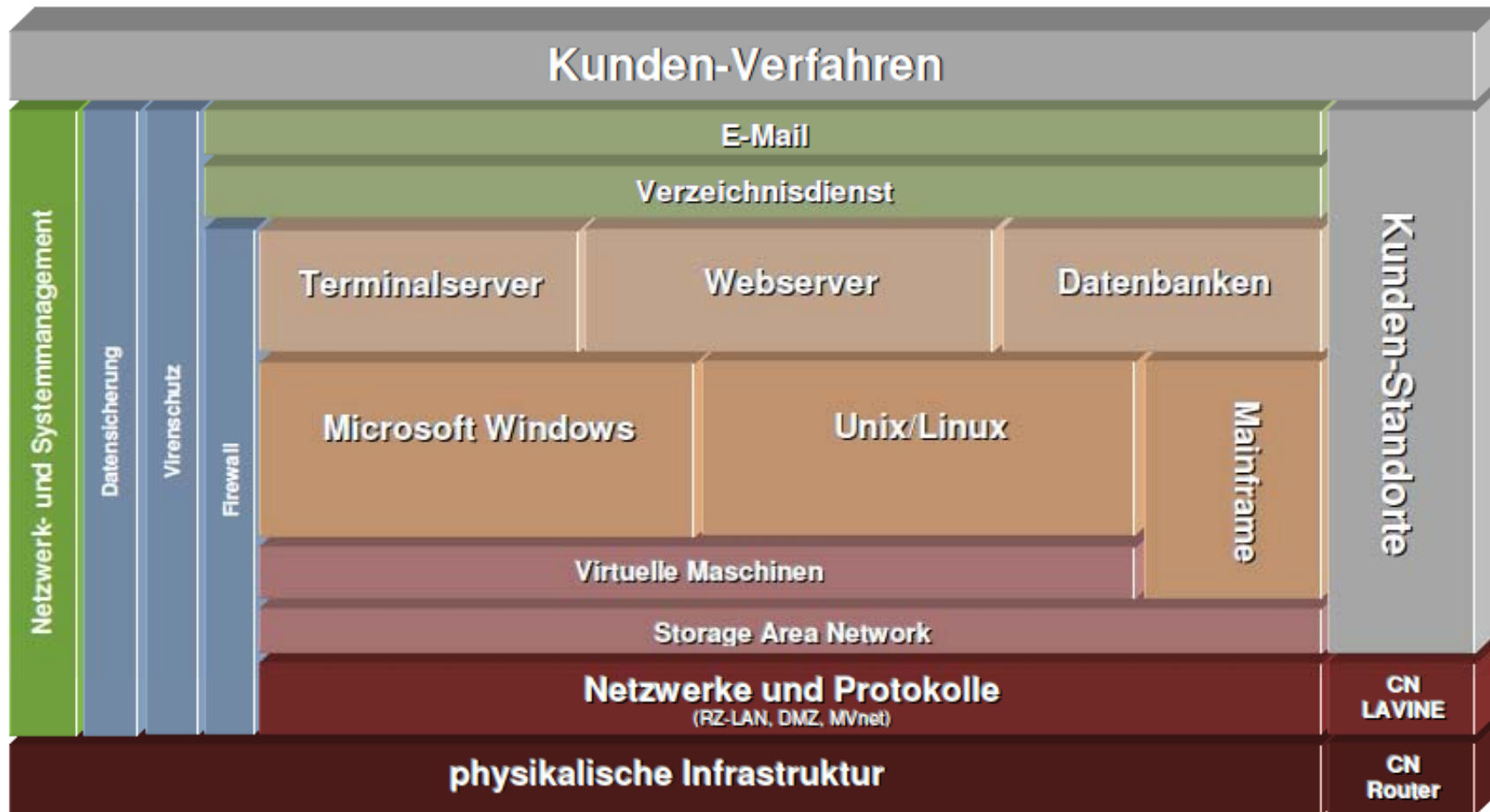
- innerhalb des zu zertifizierenden Bereichs (Informationsverbund) liegen alle Infrastrukturservices des DVZ. Hierzu zählen z.B. der Betrieb von:
 - Netzwerken inkl. CN LAVINE
 - Servern bis Betriebssystemebene
 - Datenbanken und Webservern
 - Firewall, Virenschutz und Datensicherung
 - Verzeichnis- und E-Mail-Diensten

- außerhalb des zu zertifizierenden Bereichs liegen alle Geschäftsservices, also alle kundenindividuellen Fachverfahren

- weiterhin befindet sich keine IT-Infrastruktur an Kundenstandorten im Zertifizierungsverbund



Abgrenzung des Informationsverbunds ...





- Ziel ist die Herstellung einer IT-Grundschutz-konformen Basis der Infrastrukturservices:
 - Datensicherung, DNS, ESX-Host, ESX-Management, VPN, Viruswall, Softwareverteilung, Patch-Management, Proxy, Firewall-Management, E-Mail, IT-Management
- der Kunde erhält eine „ABC“-Absicherung für „normalen“ Schutzbedarf
- **Grundsätzliche Zertifizierbarkeit des Informationsverbunds wurde vom BSI am 25.05.2011 bestätigt!**
- höherwertige Anforderungen (z. B. Z-Maßnahmen) werden auf Kundenwunsch umgesetzt
- für ein einheitliches Sicherheitsniveau sollte der Kunde ein eigenes organisationsweites ISMS etablieren



- Ausschreibung – Durchführung durch externen Dienstleister
- Erstellen eines gemäß IT-Grundsatz gruppierten Netzplans
 - Gruppieren der IT-Systeme im betrachteten Informationsverbund
 - Ermitteln der technischen und logischen Netzwerkstruktur
 - Dokumentation der Ergebnisse in einem gruppierten Netzplan
- Bewertung der Netzwerkinfrastruktur im betrachteten Bereich
 - Prüfung, ob die betrachtete Infrastruktur dem Stand der Technik und allgemeinen sowie speziellen Sicherheitsanforderungen des BSI entspricht.
- Ergebnisbericht mit Architekturermängeln, gefundenen Sicherheitslücken und Vorschlägen für Gegenmaßnahmen
- Vorstellung der Ergebnisse in einem Workshop in der DVZ-MV GmbH
 - Projektlaufzeit: 15 Tage



Modellierung ...

The screenshot shows the GSTOOL software interface. The main window title is "GSTOOL - [10.4.124.1\gsservermv : BSIDB_V47_RZ_ZERT]". The menu bar includes "Datei", "Bearbeiten", "Ansicht", "Extras", "Datenbank", "Fenster", and "Hilfe". The toolbar contains icons for "Neu", "Öffnen", "Speichern", "Löschen", "Aktualisieren", "Filter", "Modell", "Ansicht", "Kataloge lokal", "Kataloge online", and "Navigator".

The left sidebar contains several icons and labels: "Stammdaten", "Struktur Zielobjekt", "Modellierung", "Risikoanalyse", "Berichte", and "IT-Grundschutz benutzerdefiniert".

The main workspace displays a tree view of the project structure. The root node is "st() Zertifizierung_Rechenzentrum_DVZ_M-V_GmbH". Underneath, there are several sub-nodes, including "s- Gebäude", "s- Haus_A", "s- Haus_B+D", "s- Haus_C", "s- Haus_E", "s- Haus_G", "s- Raum", "s- IT-System", and a list of various IT assets such as "Client-PC_Windows_XP", "Drucker_Kopierer_BK", "Firewall_Cisco", "Firewall_Juniper", "Laptops_Windows_XP", "Mainframe", "Mobiltelefone", "Router_Switche_CN", "Router_Switche_RZ", "SAN_DS4700", "SAN_DX80", "SAN_EVA", "SAN_XP128", "Server_IRIX", "Server_Linux", "Server_Unix", "Server_Windows_2000", "Server_Windows_2003", "Server_Windows_2008", "Smartphones", and "Virtualisierung_Datenbankserver".

On the right side, there is a table titled "Liste der Zielobjekte". The table has four columns: "Kürzel", "Name", "Erläuterung", and "Erfa".

Kürzel	Name	Erläuterung	Erfa
Besprechungsräum...	Besprechungs...		ipsc
Büroraum-Adm	Büroraum-Admi...		ipsc
Büroraum-A	Büroraum-Allge...	Hiermit sind alle...	ipsc
Datensicherungsraum	Datensicherung...		ipsc
EtagenverteilerH_A...	Etagenverteiler...		ipsc
Hauseinspeisung	Hauseinspeisung		ipsc
Häuslicher_AP	Häuslicher_Arb...		ipsc
Medienraum	Medienraum		ipsc
Mobiler_Arbeitsplatz	Mobiler_Arbeits...		ipsc
Räume_H_E	Räume_Haus_E		ipsc
Rechenzentrum_22...	Rechenzentrum...		ipsc
RZ_Haus_C	Rechenzentrum...		ipsc
Safes_Datenträ...	Safes_Datenträ...		ipsc
Server-Test-Räume	Server-Test-Rä...	Hierzu zählen al...	ipsc
WBZ	Weiterbildungsz...		ipsc

The status bar at the bottom shows "Standard", "ipschulz", "10.4.124.1\gsservermv", "BSIDB_V47_RZ_ZERT", and "V 4.7.4715 / DB 4.47002 / MD 11".



■ Terminplanung

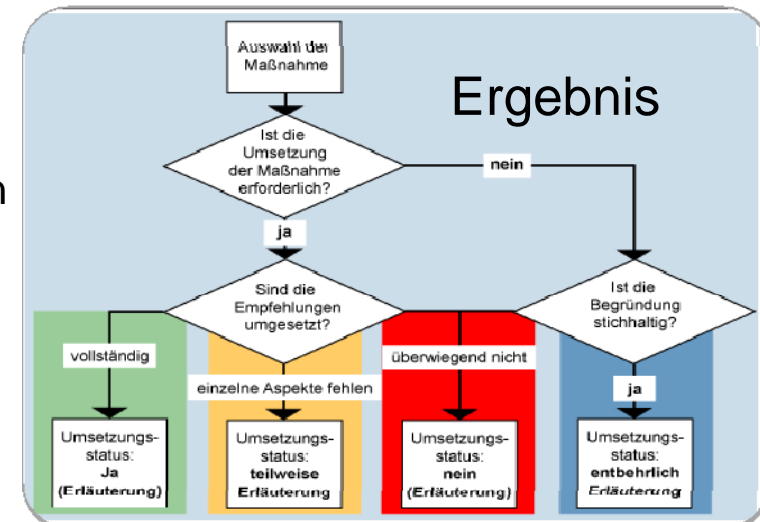
- Ermittlung der Ansprechpartner
- 5 Berater und 62 zu befragende Personen
- ca. 70 Termine in 50 Tagen

■ Vorbereitung

- Informationsveranstaltung für alle beteiligten Mitarbeiter
- Darstellung der Vorgehensweise
- Wichtig: Hinweis, dass keine persönliche Leistungsbewertung erfolgt!
- Mitarbeiter sollen auch selbst Fragen stellen
- Zur Verfügungstellung der IT-Grundschutzbausteine

■ Nachbereitung

- Zusendung der Ergebnisberichte



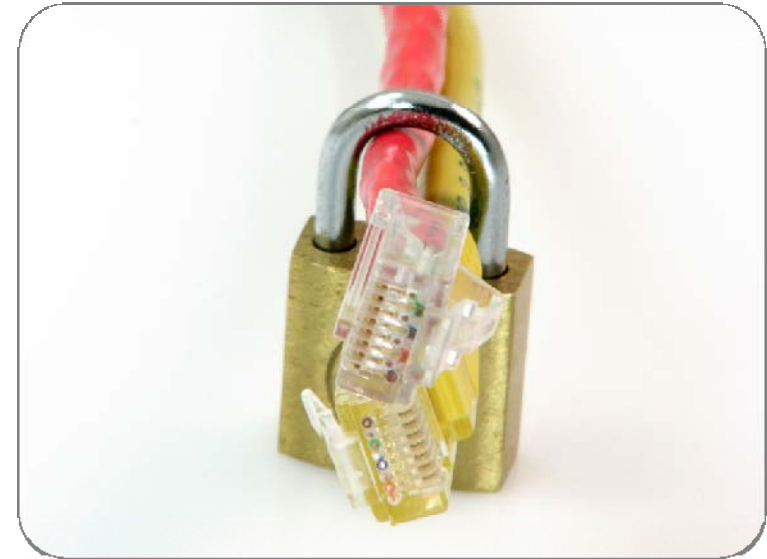


- Vorteile bei der Einbindung externer Dienstleister
 - objektivere Sichtweise – Verhinderung von Betriebsblindheit
 - größere Akzeptanz der Ergebnisse im Haus
 - breiteres und tieferes Know-how
 - Erfahrung hilft bei Interpretation der Maßnahmentexte





- Ergebnisse/Erkenntnisse
 - Vieles Standardkonform aber ...
Es gibt Defizite!
 - infrastrukturell herrscht ein
Umsetzungsgrad von fast 90% !!!
 - die gelebte Sicherheit ist größer als
die dokumentierte Sicherheit
 - hauptsächlich fehlt es an
dokumentierten Regelungen und
Konzepten
 - Verantwortlichkeiten müssen klarer
dokumentiert werden
 - technische Lücken kann ich hier
nicht nennen ...





- Konsolidierung der defizitären Maßnahmen in Arbeitspakete (Projekt-Portal)
- Benennung von sechs Team-Managern (TM) zu folgenden Bereichen:
 - Informationssicherheitsmanagement
 - Querschnittsthemen
 - Sicherer Serverbetrieb
 - Netzwerksicherheit
 - Notfallmanagement
 - Virenschutz
- Aufwandsabschätzung durch die TM und Terminplanung
- Realisierung durch die verantwortlichen Mitarbeiter
- Abnahme der Ergebnisse durch den Informationssicherheitsmanager



- Anpassung der Fertigstellungstermine nach Aufwand und Ressourcen
- hoher Sach- und Personal-Aufwand
- Realisierung der Maßnahmen „neben“ dem Betrieb und Kundenprojekten
- Konsolidierung von verfahrensspezifischen Maßnahmen und Anforderungen auf einen DVZ-einheitlichen Standard
- Alle Maßnahmen müssen aufrechterhalten und gelebt werden





Zertifizierungs-Ablauf ...

Mai 2012

- Realisierung A-Maßnahmen
- Auditor-Testat Einstiegsstufe

September 2012

- Realisierung B/C-Maßnahmen
- ISO 27001/IT-Grundschutz-Zertifikat

September 2013

- 1. Überwachungs-Audit

September 2014

- 2. Überwachungs-Audit

September 2015

- Re-Zertifizierung



- Das DVZ als stärkstes Glied in einer "schwachen" Kette?
 - Für ein einheitliches Sicherheitsniveau müssen alle am Verfahren beteiligten Organisationen ein ISMS betreiben
 - Absicherung der Kunden(-Standorte)
 - Erstellung eines Sicherheitskonzepts für den gesamten Kundenstandort
 - Definition von Schnittstellen zwischen DVZ- und Kunden-ISMS
 - Realisierung und regelmäßige Prüfung der Sicherheitsmaßnahmen





Fragen und Diskussionen



www.dvz-mv.de

JAN-PETER SCHULZ

Telefon: +49 (0) 385 4800 513

Mobil: +49 (0) 175 4320737

E-Mail: j.schulz@dvz-mv.de

GEMEINSAM VISIONEN VERWIRKLICHEN.

www.dvz-mv.de

VIELEN DANK FÜR DIE AUFMERKSAMKEIT.

