



Architect of an Open World™

Vom Datenfriedhof zum Compliance-Archiv

Was sagt der österreichische Gesetzgeber?

LIBERATE IT

Agenda

- Vorstellung
- Archiv = Archiv ?
- Richtlinien & Gesetze
 - Basel 2
 - SOX
 - UGB
 - UstG
- Ein Blick zum Nachbarn
- Beweiskraft von E-Mails
- Begriffe



Vorstellung

Eduard Mantl

Consultant

BULL GmbH

Lemböckgasse 49A

A-1230 Wien

email: e.mantl@bull.at

web : <http://www.bull.at>



Berufliche Laufbahn:

Techniker & Consultant,

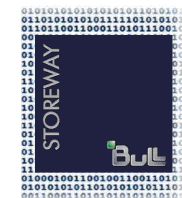
IT-Verantwortlicher,

Senior Systems Engineer,

Projektmanager

Autor des Buches “Holistische IT-Security”

www.holistische-it-security.at



Archiv = Archiv ?

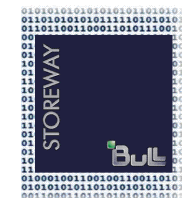
- Warum archivieren?
 - Reduktion der Datenmenge auf dem Primär-Storagesubsystem und Auslagerung auf günstige Sekundär-Storage
 - Entlastung des E-Mailservers durch Transfer und Archivierung der älteren Daten auf ein anderes System
 - Rasches Auffinden von Informationen durch übergreifende Suchfunktion (E-Mail, Files& Archiv)
 - Compliance-Anforderungen



Archiv = Archiv ?

- Warum archivieren?
 - Reduktion der Datenmenge auf dem Primär-Storagesubsystem und Auslagerung auf günstige Sekundär-Storage
 - Entlastung des E-Mailservers durch Transfer und Archivierung der älteren Daten auf ein anderes System

=> Kosten senken



Archiv = Archiv ?

- Warum archivieren?
 - Rasches Auffinden von Informationen durch übergreifende Suchfunktion (E-Mail, Files& Archiv)

=> Human Ressourcen entlasten

=> Kosten senken



Archiv = Archiv ?

- Warum archivieren?
 - Compliance-Anforderungen



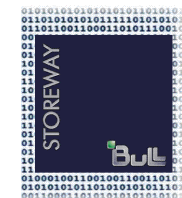
=> Gesetze und Richtlinien (UGB, SOX, UStG, ...)

=> verursacht Kosten

Archiv = Archiv ?

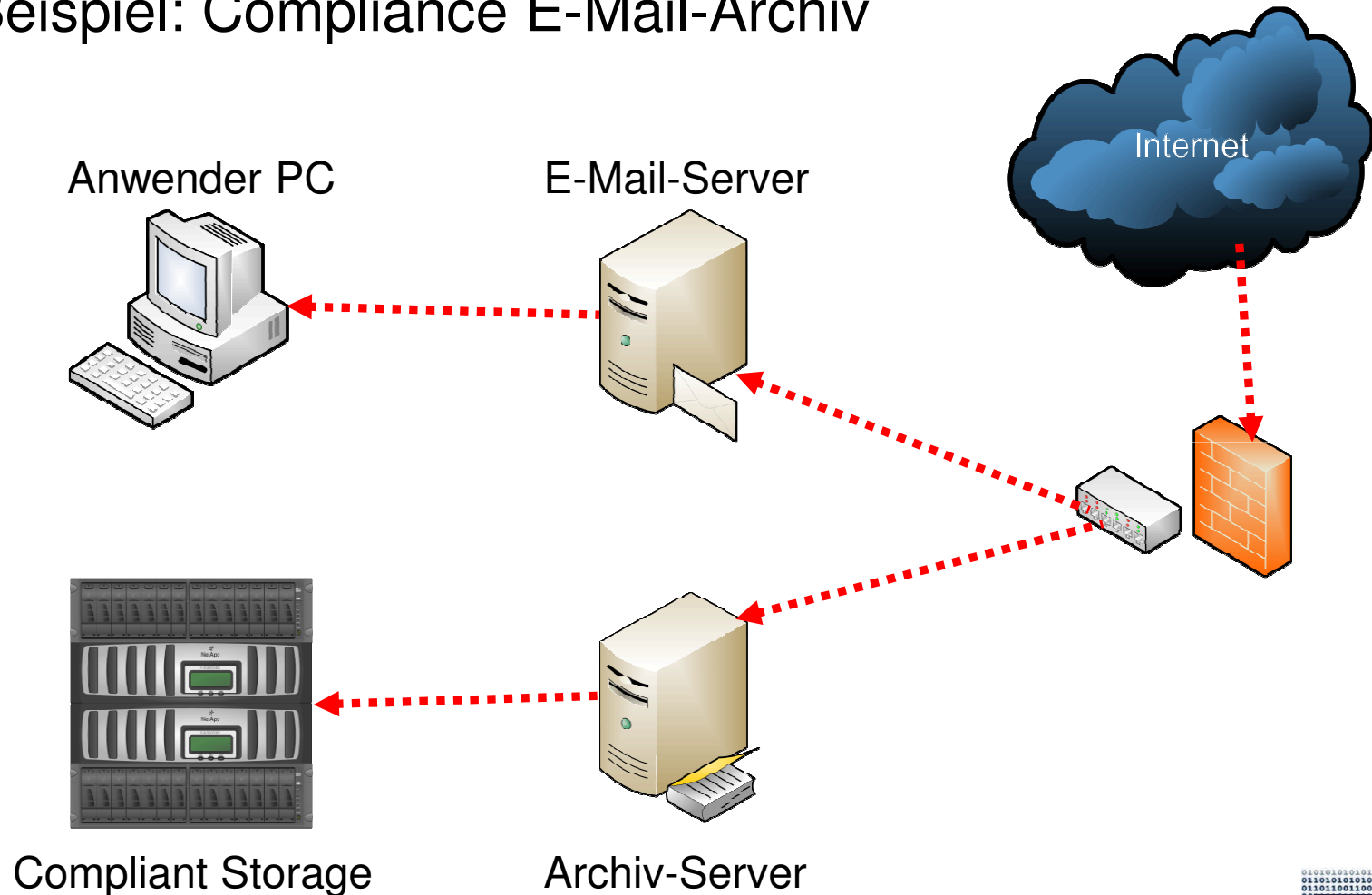
- Archiv zum Entlasten von Ressourcen
 - Entlastet teure Server und Stagesubsysteme
 - Erleichtert das Auffinden von Dokumenten
 - Reduziert Kosten

- Archiv zum Erfüllen von Compliance-Richtlinien
 - Unveränderbare Vorhaltung bis zum Ablauf der gesetzlichen Aufbewahrungsfrist
 - Für „Compliance“ ist auch eine „compliant Storage“ und entsprechende interne Abläufe nötig – keine Software für sich genommen kann „compliant“ sein!
 - Verursacht Kosten



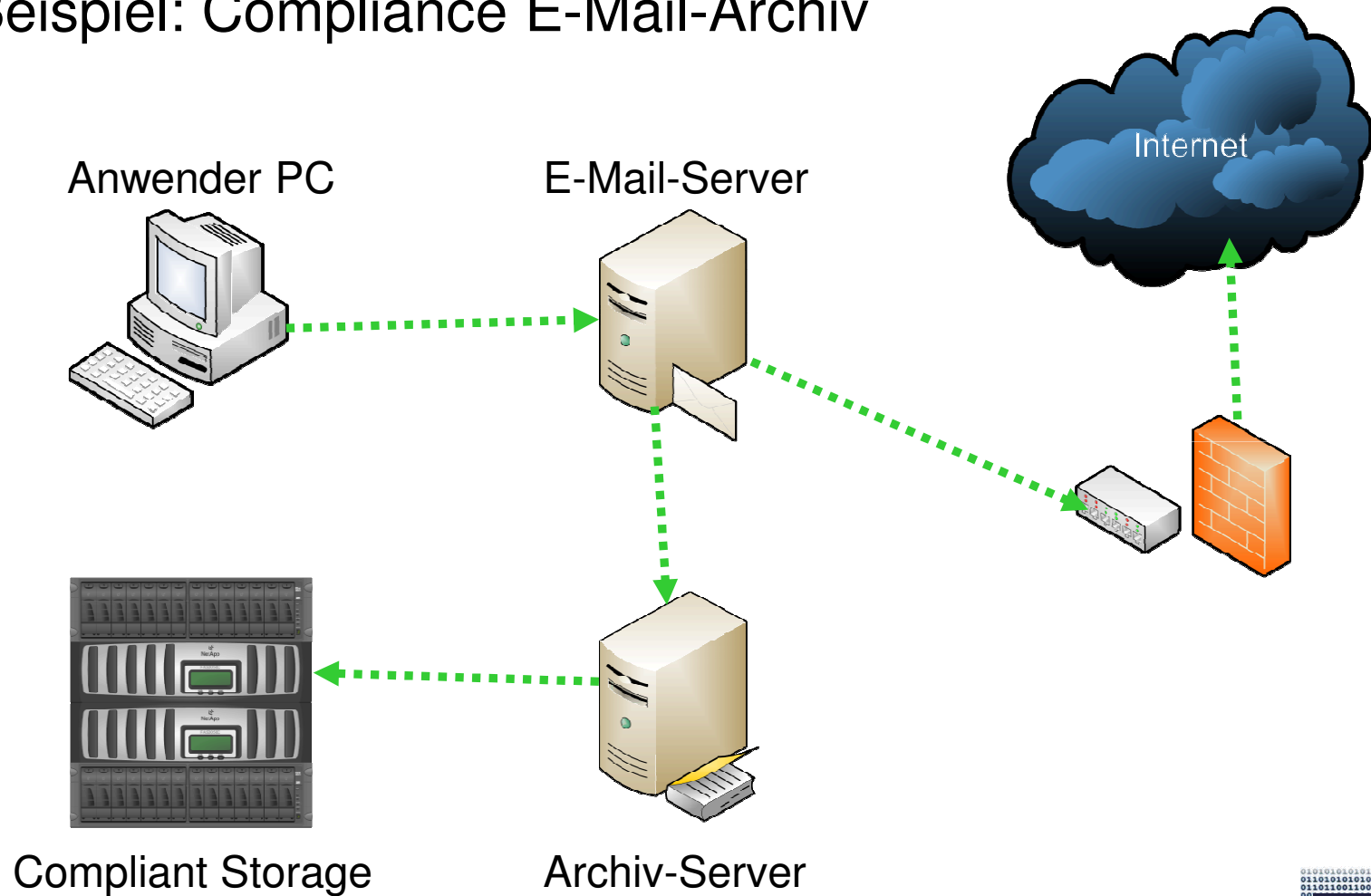
Archiv = Archiv ?

- Beispiel: Compliance E-Mail-Archiv



Archiv = Archiv ?

- Beispiel: Compliance E-Mail-Archiv



Richtlinien & Gesetze

- Basel 2
- SOX
- UGB
- UstG



Richtlinien und Gesetze – Basel 2

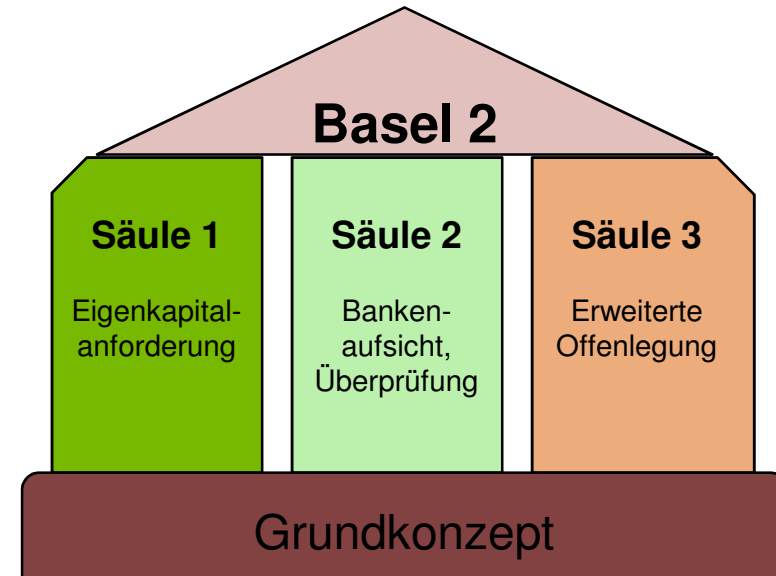
- Richtlinie 2006/48/EG und 2006/49/EG = Basel 2

- Regeln gelten für

- Kreditinstitute
- Finanzdienstleistungsinstitute

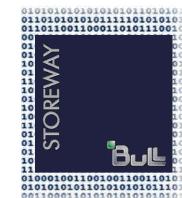
- Ziele

- Sicherung einer angemessenen Eigenkapitalausstattung
- Einheitliche Bedingungen für Kreditvergabe und –handel
- Ausrichtung der Eigenkapitalausstattung am tatsächlichen Risiko



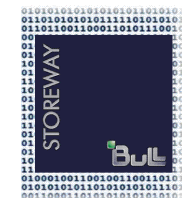
Richtlinien und Gesetze – Basel 2

- Risikomanagement nach Basel 2 ???
 - Basel 2 fordert Risikomanagement (in erster Linie von den Banken), beschreibt aber nicht wie dieses auszusehen hat
 - Risikomanagement wird in ISO 27001 behandelt
 - Wer ISO 27001 erfüllt, hat auch mit Basel 2 keine Probleme
- Auswirkungen auf Unternehmen außerhalb der Finanzdienstleistungs-Branche ???
 - Juristisch: Keine
 - Schlechter bewertete Bonität und dadurch höhere Kreditzinsen
 - Im Extremfall kein Kredit

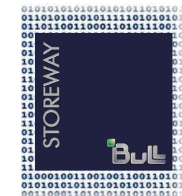


Richtlinien und Gesetze – SOX

- Sarbanes-Oxley-Act (auch SOX oder SOA)
- US-Amerikanisches Gesetz gilt für
 - US-Amerikanische börsennotierte Unternehmen
 - Ausländische Unternehmen die an US-Börsen gelistet sind
 - ... deren Tochterunternehmen
- Ziele
 - Verbindliche Regelung der Unternehmensberichterstattung
 - Wiederherstellung des Vertrauens bei Anlegern

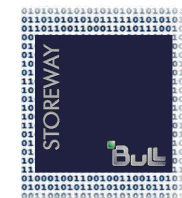


- Die wichtigsten Bestimmungen
 - **Section 302:** Die Richtigkeit der Bilanzen muss vom Geschäftsführer und Leiter der Finanzabteilung beglaubigt werden. Die Finanzdaten müssen fehlerfrei und vollständig sein
 - **Section 404:** Der Geschäftsführer, Leiter der Finanzabteilung und Abschlussprüfer müssen die Effektivität interner Kontrollen bestätigen. Unternehmen müssen die Effektivität der Kontrollen erhalten, überwachen und entsprechende Berichte erstellen
 - **Section 409:** Unternehmen müssen eine wesentliche Veränderung ihrer Finanzsituation in Echtzeit offen legen. Verstöße oder Abweichungen, die auf mögliche erhebliche Veränderungen hinweisen, müssen frühzeitig erkannt werden.
 - **Section 802:** Unternehmen müssen die Unterlagen der Abschlussprüfung aufbewahren und schützen. In Übereinstimmung mit den Unternehmensrichtlinien muss sichergestellt werden, dass die Unterlagen verfügbar sind und nicht verändert werden. Unternehmen müssen ausreichende Sicherheitsmaßnahmen ergreifen, um die Einhaltung dieser Bestimmungen zu gewährleisten.



Richtlinien und Gesetze – SOX

- Daraus folgt ...
 - Alle Unternehmensprozesse in denen Zahlen für die Finanzberichterstattung entstehen, müssen mit Kontrollen versehen werden
 - Geschäftsrelevante Unterlagen - auch E-Mails – müssen revisionssicher sein
 - CEO und CFO müssen die Ordnungsmäßigkeit einer Bilanz und die Wirksamkeit der Kontrollen bestätigen und haften persönlich
- Auswirkungen auf Unternehmen außerhalb USA
 - Juristisch: Keine (US-Gesetz gilt in den USA)
 - Für Aktiengesellschaften: Delisting von US-Börsen



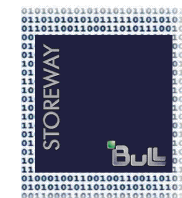
Richtlinien und Gesetze – UGB

- §190

- (5) Der Unternehmer kann zur ordnungsmäßigen Buchführung und zur Aufbewahrung seiner Geschäftsbriefe (§ 212 Abs. 1) Datenträger benutzen. Hierbei muss die inhaltsgleiche, vollständige und geordnete ... Wiedergabe bis zum Ablauf der gesetzlichen Aufbewahrungsfristen jederzeit gewährleistet sein ...

- §212

- (1) Der Unternehmer hat seine Bücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse samt den Lageberichten, Konzernabschlüsse samt den Konzernlageberichten, empfangene Geschäftsbriefe, Abschriften der abgesendeten Geschäftsbriefe und Belege für Buchungen in den von ihm gemäß § 189 Abs. 1 zu führenden Büchern (Buchungsbelege) sieben Jahre lang geordnet aufzubewahren; darüber hinaus noch solange, als sie für ein anhängiges gerichtliches oder behördliches Verfahren, in dem der Unternehmer Parteistellung hat, von Bedeutung sind.



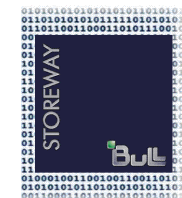
Richtlinien und Gesetze – UGB

- §190

- (5) Der Unternehmer kann zur ordnungsmäßigen Buchführung und zur Aufbewahrung seiner Geschäftsbriefe (§ 212 Abs. 1) Datenträger benutzen. Hierbei muss die **inhaltsgleiche, vollständige und geordnete ... Wiedergabe bis zum Ablauf der gesetzlichen Aufbewahrungsfristen jederzeit gewährleistet** sein
...

- §212

- (1) Der Unternehmer hat seine Bücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse samt den Lageberichten, Konzernabschlüsse samt den Konzernlageberichten, **empfangene Geschäftsbriefe, Abschriften der abgesendeten Geschäftsbriefe** und Belege für Buchungen in den von ihm gemäß § 189 Abs. 1 zu führenden Büchern (Buchungsbelege) **sieben Jahre lang geordnet aufzubewahren**; darüber hinaus noch solange, als sie für ein anhängiges gerichtliches oder behördliches Verfahren, in dem der Unternehmer Parteistellung hat, von Bedeutung sind.



- § 216

- Wer Eintragungen oder Aufbewahrungen ... vorgenommen hat muß ... auf seine Kosten innerhalb angemessener Frist diejenigen Hilfsmittel zur Verfügung stellen, die notwendig sind, um die Unterlagen lesbar zu machen, und, soweit erforderlich, die benötigte Anzahl ohne Hilfsmittel lesbarer, dauerhafter Wiedergaben beibringen.



Richtlinien und Gesetze – UstG

- Auch im UstG werden Aufbewahrungsfristen geregelt
- Z.B.: § 11
 - (2) ... Stellt der Unternehmer Rechnungen ... aus, so hat er eine Durchschrift oder Abschrift anzufertigen und sieben Jahre aufzubewahren; das gleiche gilt sinngemäß für Belege, auf die in einer Rechnung hingewiesen wird. ... Die Echtheit der Herkunft und die Unversehrtheit des Inhalts der auf elektronischem Weg übermittelten Rechnungen muss für die Dauer von sieben Jahren gewährleistet sein.

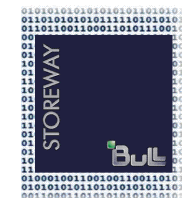


- Auch im UstG werden Aufbewahrungsfristen geregelt
- Z.B.: § 11
 - (2) ... Stellt der Unternehmer Rechnungen ... aus, so hat er eine Durchschrift oder Abschrift anzufertigen und sieben Jahre aufzubewahren; das gleiche gilt sinngemäß für **Belege, auf die in einer Rechnung hingewiesen wird. ... Die Echtheit der Herkunft und die Unversehrtheit des Inhalts der auf elektronischem Weg übermittelten Rechnungen** muss für die Dauer von sieben Jahren gewährleistet sein.



Ein Blick zum Nachbarn

- In Deutschland wird vieles schon genauer geregelt
 - **Grundsätze** basieren auf Regeln die sich aus Wissenschaft, Rechtsprechung, Praxis und Empfehlungen von Wirtschaftsverbänden ergeben
 - **GOB** – Grundsätze ordnungsgemäßer Buchführung
 - **GoBS** – Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme
 - **GDPdU** - Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen



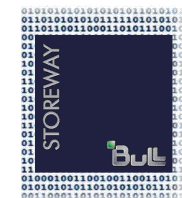
Beweiskraft von E-Mails

- E-Mails gelten als Schriftstück und werden prinzipiell zur Beweisführung zugelassen
(freie Beweiswürdigung § 272 ZPO)

- Jedoch nicht in jeder Form anerkannt

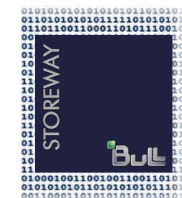
Entscheidung des Amtsgerichtes Bonn über ein ausgedrucktes E-Mail (Urteil vom 25.10.2001 – 3 C 193/01 – Deutsche Entscheidung, jedoch auch in Österreich denkbar)

... Es ist allgemein bekannt, daß E-Mail-Daten manipulierbar sind. Selbst wenn die E-Mails grundsätzlich vom Beklagten abgesandt worden sein sollten, wäre es möglich, daß einzelne Worte oder einzelne Sätze von Dritten abgeändert worden sind. Soweit kann diesen vom Kläger vorgelegten E-Mail-Ausdrucken keinerlei Beweiswert beigemessen werden ...



Begriff - Revisionsicher

- Der Begriff “Revisionsicher” kommt in keinem Gesetz vor
- Was bedeutet “Revisionsicher” – sicher vor der Revision?
- Revisionsicherheit im IT-Umfeld ist ...
 - Nachvollziehbar
 - Vollständig
 - Unveränderbar
 - Verfälschungssicher
 - (Datenbankgestützt) Wiederauffindbar



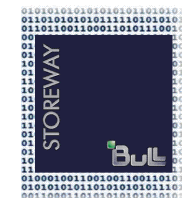
Begriff - Stand der Technik

- Der Gesetzgeber verordnet keine konkreten Techniken, sondern formuliert abstrakte Anforderungen
- Techniken entwickeln sich permanent weiter, Gesetze bestehen oft für Jahrzehnte
- Die realen Anforderungen ergeben sich aus der Interpretation der Gesetze
- Daher der Begriff **“Stand der Technik”** oder **„Stand der technischen Möglichkeiten“** (siehe z.B. §14 DSGVO2000)
- Bei der Interpretation eines Gesetzes wird der Stand des technisch machbaren herangezogen, auch wenn das Gesetz ev. schon viel älter ist, als die heute üblichen technischen Lösungen



Begriff – Sorgfalt eines ordentlichen Unternehmers

- § 347 UGB
 - Wer aus einem Geschäft, das auf seiner Seite unternehmensbezogen ist, einem anderen zur Sorgfalt verpflichtet ist, hat für die **Sorgfalt eines ordentlichen Unternehmers** einzustehen.



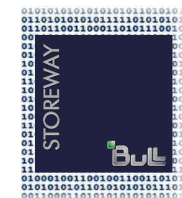
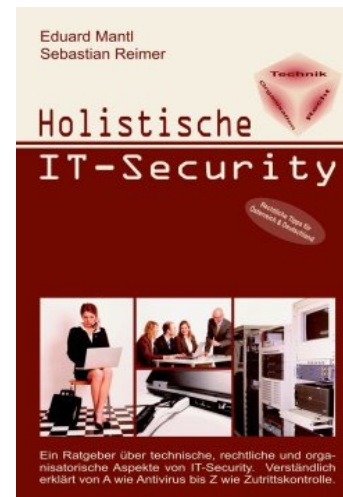
Buch Empfehlung

Holistische IT-Security

Ein Ratgeber über
technische, rechtliche
und organisatorische Aspekte

ISBN: 978-3-85028-450-9

www.holistische-it-security.at





Architect of an Open World™

LIBERATE IT