HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Die Pflicht zur revisionssicheren E-Mail-Archivierung

Peer Heinlein

Christian Meissner

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Die rechtlichen Vorschriften

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Rechtliche Grundlagen

Handels-/Geschäftsbriefe

- es existierten schon immer Regelungen zur Archivierung von Handels-, bzw. Geschäftsbriefen
- Je nach Rechtsform unterschiedliche Rechtsgrundlagen:
- §37a HGB, §80 I AktienG, §35a I GmbHG und viele, viele weitere §§.

Umfaßt heute auch zweifelsfrei auch E-Mails und Fax

- Darum: Pflicht zur Archivierung geschäftlicher E-Mails
- Darum: Pflicht zu E-Mail-Signatur mit geschäftl. Mindestinformationen

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Geschäftsbriefe und Handelsbriefe

Geschäftsbriefe: Briefe zwischen Geschäftspartnern (auch zwischen Geschäftsmann und Privatperson!)

- Untermenge davon: Der Handelsbrief ist jeder Brief, der zur
  - Vorbereitung
  - Durchführung
  - Abschluss
  - oder Rückabwicklung
- eines Handelsgeschäftes dient.

Beispiele

- Bestellung & Rechnung
- Aber auch: Infoanfrage, Angebot, Katalogbestellung
- Aber auch: Liefertermine, weitere Absprachen, Reklamationen

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Firmeninterner Schriftverkehr

Firmeninterner Schriftverkehr (zwischen Mitarbeitern) ist kein Geschäfts- oder Handelsbrief.

Keine Archivierung!

(Ausnahmen in Konzern-Konstrukten möglich!)

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Archivierungszeiten nach HGB

Sind an verschiedenen Stellen geregelt, sagen jedoch übereinstimmend:

Auf zehn Jahre revisionssicher zu archivieren:

- Bücher und Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, die Eröffnungsbilanz sowie die zu ihrem Verständnis erforderlichen
- Buchungsbelege
- Zollanmeldungen & Co

Alles andere sechs Jahre archivieren!

- Empfangene und abgesandte Geschäfts-/Handelsbriefe

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Derer Rechtsgrundlagen gibt es viele...

Handelsgesetzbuch (HGB) §§238, 239, 257

Abgabenordnung (AO) §147

Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)

Grundsätze ordnungsgemäßer DV-gestützter Speicherbuchführung (GoBS)

Umsatzsteuergesetz (UStG)

Bundes- und Landesdatenschutzgesetze (BDSG, LDSG)

Signaturgesetz §15

Gesetz zur Kontrolle und Transparenz im Unternehmen (KonTraG)

Sarbanes-Oxley-Act (SOX)

Basel II-Richtlinie

Prinzipiell sogar: Art. 20 III Grundgesetz (Rechtsstaatlichkeit der Verwaltung)

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Archivierungspflichten der öffentlich-rechtlichen Hand

Ist prinzipiell nicht von HGB, GmbHG, AktienG, AO etc. erfaßt.

Aber: Wirtschaftlicher Zweckbetrieb

- Wer sich wie ein Unternehmer generiert wird wie ein Unternehmer behandelt

Auskunftsansprüche von Bürger und Dritten

- VerwaltungsverfahrensG (VwVfG), SGB X, BDSG, InformationsfreiheitsG (IFG)

Aufsichtsbehörden

- Kommunal-/Fachaufsicht, Rechnungsprüfungsbehörden

Rechtsstaatlicher Gesetzesvollzug

- Erfordert umfangreiche Dokumentation => Eingang der E-Mails in Akte?

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Im Ergebnis...

Egal welche Rechtsgrundlage:

Geschäftliche E-Mails müssen 6, bzw. 10 Jahre revisionssicher elektronisch auswertbar archiviert werden.

Auch Auswirkungen auf öffentlich-rechtliche Hand!

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Die revisionssichere Archivierung

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Wie darf/muss gespeichert werden?

- Originäres elektronische Daten müssen weiterhin elektronisch archiviert werden
  - Keine Speicherung in Papierform (Ausdruck)
- Elektronisch auswertbare Daten müssen elektronisch auswertbar bleiben
  - Anhänge müssen erhalten bleiben in originärem Format (z.B. Excel-/OO-Tabelle)
  - Keine Speicherung als PDF o.ä. (Konvertierung)

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Was bedeutet „revisionssichere“ Archivierung?

Kein nachträglicher Verlust der Daten

Keine nachträgliche (unbemerkte) Veränderung der Daten

Datenveränderungen müssen rückgängig zu machen sein

Ergo: Keine Manipulation durch Admin/root, Geschäftsführung oder Hacker darf möglich sein.

Root-Passwortschutz für die Datenbank o.ä. ist nicht ausreichend!

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Weitere Anforderung an das Archiv

- Daten müssen in angemessener Zeit wieder verfügbar gemacht werden können
  - Suchfunktion, passende Medien
- Migration auf neue Speichertechnologien muß möglich sein
  - Berücksichtigung von Volumen-Wachstum
- Keine Vorschriften zur Umsetzung der Revisionssicherheit oder Speicherart
- Wünschenswert: Hilfsmittel zur Einhaltung der Aufbewahrungszeiten

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Archivierungskonzepte im Vergleich

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Denkbare Konzepte für eine E-Mail-Archivierung

Manuelle Archivierung auf dem Nutzer-Desktop oder Server

Automatische Archivierung auf dem (Groupware-) Server

Automatische Archivierung durch SMTP-Proxy vor dem Server

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Manuelle Archivierung durch den Nutzer/Mitarbeiter

- User entscheidet wann und was archiviert wird
  - Nutzer hat keinerlei Rechtsverständnis von Geschäftsbriefen und der Notwendigkeit/Verpflichtung
  - In der Praxis immense Lücken in der Archivierung
  - Persönlicher Archiv-Ordner eines Nutzers: Keinesfalls revisionssicher.
- Keine Unternehmensleitung wird sich darauf verlassen können
- Hohe juristische und finanzielle Risiken für Unternehmen
- Auch hohe persönliche Risiken für den Unternehmer!

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Archivierung auf dem (Groupware-) Server

Meistens durch ein Plugin in der Serversoftware

+ Zentrale Administration über das GW-Admininterface
+ Speicherung der Daten in der GW-Datenbank
+ Oft gute Einbettung im Desktop-Client wie Outlook

Archiv steht und fällt mit der Groupware-Software

-- Migration der GW kaum mehr möglich
-- Ansonsten paralleler Weiterbetrieb der Groupware für weitere 10 Jahre nötig!
-- Starke Abhängigkeit zum Softwarehersteller

Welche Software haben Sie eigentlich 1999 eingesetzt?

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Archivierung durch einen SMTP-Proxy

In- und Outbound-Verkehr wird erfasst

Interner Verkehr eh unerwünscht im Archiv.

Flexible Speicherung in Dateisystem oder Datenbank

Konzept je nach Hersteller der Archivsoftware

Zugriff für User per Webinterface oder per IMAP-readonly

--: Oft nicht so gute GUI-Implementierung auf dem Desktop

Aber: Archiv ist vorrangig für Betriebsrevision da, nicht für Endnutzer!

Unabhängig von jeder Groupware

+++: Archiv bleibt beim Wechsel problemlos erhalten!

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Die Probleme in der Praxis

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Revisionssicherheit: Ich bin root, ich kann alles?

- Admin/root darf nicht mehr verändern können
- Kryptographische Signierung
  - Zuhilfenahme signierter Zeitstempel akkreditierter Dienste (SigG)
  - Auch root kann nachträglich nicht mehr manipulieren und rückdatieren!
- WORM (write once read many)
  - Hardwarehersteller bieten große einmalig beschreibbare Storage-Systeme an
  - Hersteller garantiert die Unveränderbarkeit der Daten

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Anforderung an die Kryptographie der Revisionssicherheit

Was heute noch „sicher“ ist, gilt morgen als geknackt.

- Beispiel: MD5 schon heute zu unsicher.
- Eine MD5-Signatur von 2005 ist 2015 nichts mehr wert.

Ergo: Nachsignieren des Datenbestandes mit neueren Algorithmen bevor ursprüngliche Algorithmen unsicher werden

- Mehrere übereinanderliegende Signatur-Container stellen Revisionssicherheit auch dann her, wenn ursprünglicher Algorithmus obsolet ist.
  SHA256 (MD5 (E-MAIL))

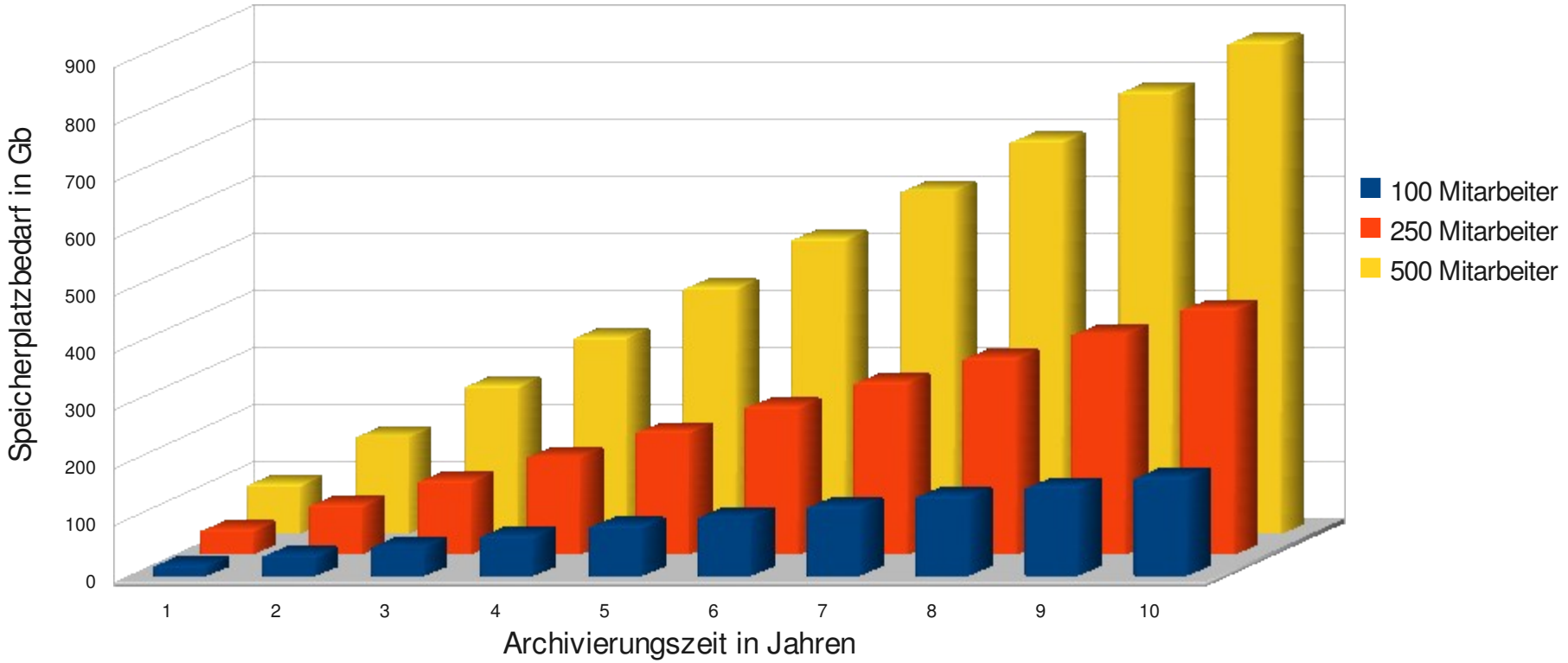
Ein Mailarchiv als Eigenbaulösung?

- Ganz so einfach ist es also doch nicht.
- Und Vorsicht: Kryptographie selber bauen hat noch nie funktioniert.

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Problem: Der Speicherverbrauch (1)

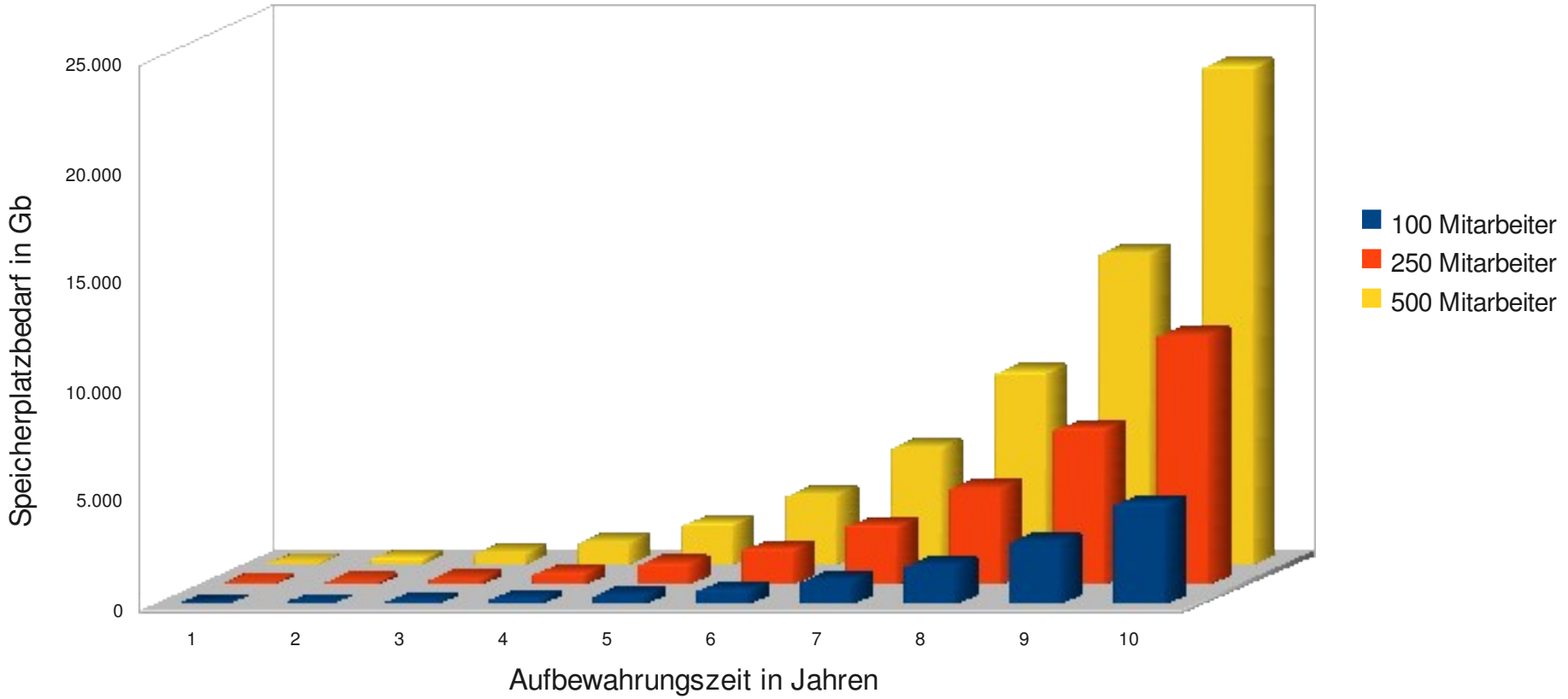
Speicherplatzbedarf
bei einer E-Mailgröße von 25Kb und 20 Mails pro Tag
Ohne jegliche Steigerung



HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Problem: Der Speicherverbrauch (2)

Speicherplatzbedarf
bei einer E-Mailgröße von 25Kb und 20 Mails pro Tag
sowie einer Steigerung an Größe und Menge von jeweils 20% jährlich



HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Probleme bei privater Nutzung von E-Mails am Arbeitsplatz

Massive Konflikte mit Datenschutz

- Persönliche E-Mails dürfen nicht ohne weiteres archiviert werden!
- Löschungsanspruch auf archivierte E-Mails?

Immense Kosten durch privater Nutzung

- Datenvolumen privater Nutzung erzeugt bei 10jähriger Archivierung immense, nicht zu rechtfertigende Kosten

Wie geschäftliche und private E-Mails trennen?

- Verbot privater Nutzung oder Umsetzung eines **richtigen** Konzeptes zu privater Nutzung unbedingt notwendig (getrennte Server, getrennte Mailadressen!)

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Praktische Probleme bei der Langzeitarchivierung

- Doppelte (und damit teure) Datenhaltung in Mailarchiv und Dokumentenmanagement-System
  - Problem: Wird Dokument im DMS eingecheckt muß es als E-Mail bereits archiviert worden sein. „Single Instance“-Speicherung sehr schwierig bzw. Aufgabe der DMS-Hersteller!
- Aufgaben-/Namenswechsel von Mitarbeitern?
  - Archivlösung muß Protokollmechanismen dafür haben
- Wann dürfen E-Mails gelöscht werden?
  - Welche E-Mails sind sechs, welche sind zehn Jahre aufzuheben?
  - Faktisch: Im Zweifel alle E-Mails 10 Jahre aufheben?!

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

E-Mail-Archivierung und Spam-/Virenschutz

Jedes Anti-Spam-System hat eine False Positives-Rate.

Wird Spam getaggt, so wird es auch getaggte „echte“ E-Mails geben.

Werden getaggte E-Mails pauschal nicht archiviert entstehen Lücken im Archiv.

Spam zu archivieren produziert zehn- bis zwanzigfaches Datenvolumen (95% Spamquote!)

Mit Blick aufs Archiv: Spam/Viren direkt ablehnen

Keine empfangene E-Mail, keine Notwendigkeit zur Archivierung.

Einziger Weg zur Vollständigkeit und damit größten Rechtssicherheit.

Ergo: Archiv wird nach Spam-/Virenfilter platziert

Ideal: Das spam-/virenfilternde Archiv oder der archivierende Spam-/Virenfilter...

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Verschlüsselte E-Mails

Problem: Schlüssel, bzw. Wissen um Passwort in 10 Jahren

Um Nachvollziehbarkeit zu gewährleisten eigentlich unverschlüsselte Archivierung der Daten nötig

Problem: Was bei Verschlüsselung auf dem Desktop?

Unproblematisch: Verschlüsselungs-Gateway vor dem Mailarchiv.

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Bevor Archivierung eingeführt werden kann

- Vor der Einführung einer Archivierung steht i.d.R. die (oft dringend überfällige) saubere Neustrukturierung des E-Mail-Verkehrs eines Unternehmens
  - Konzept zum Spam-Virenschutz
  - Private Nutzung
  - Datenschutz
  - Einhaltung sonst. rechtlicher Vorschriften
- Erst denken/planen, dann handeln/einführen!
  - Fehler können irreparable juristische Spätschäden hervorrufen
  - Fehler können hohe unnötige Folgekosten verursachen
  - Die Zeit drängt. Archivierung ist seit 1.1.2006 Pflicht.

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Folgen bei fehlender Archivierung

- Verstoß gegen Grundsätze ordnungsgemäßer Buchführung
- Unternehmen muß erhebliche wirtschaftliche Risiken attestiert werden.
  - Sinkende Kreditwürdigkeit! Keine oder teurere Kreditlinien!
  - Verstoß des Unternehmers gegen unternehmensrechtliche Vorschriften!
  - Ggf. Beweislastumkehr und ggf. steuerrechtliche Schwierigkeiten!
  - Ggf. Verstoß gegen aktienrechtliche Vorschriften! Probleme an den Börsen.

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Es sei uns erlaubt anzumerken...

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Heinlein Mailarchiv

- Auf Kundenwunsch im Rahmen unserer täglichen Consultant-Arbeit entstanden
  - Damals keine revissionssicheren interoperablen Lösungen vorhanden
- Setzt „unsere“ Vorstellungen eines Archivs um
  - Sauber: Arbeitet transparent als SMTP-Proxy
  - Gerichtsfest: Modul zur Revisionssicherheit stammt von Fraunhofer SIT
  - Offen: Arbeitet mit beliebigen (auch externen) SQL-Datenbanken zusammen
  - Alles-in-einem: Kann auch Spam-/Virenfilterung
  - Nett: Bietet Nutzern selbstständigen Zugriff auf Backup ihrer Inbox
  - Ansonsten: KISS (keep it simple and stupid) – Archiv muß rock-solid sein!
- Christian Meissner ist AP für Live-Demo oder Teststellung

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Ja, diese Folien stehen als PDF im Netz...
http://www.heinlein-support.de

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Soweit, sogut.

Fragen?

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Und nun...

Vielen Dank für's Zuhören...

Schönen Tag noch...

Und viel Spaß an der Tastatur.

Bis bald.

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Heinlein Support hilft auch bei allen Fragen rund um E-Mails:

AKADEMIE

Von Profis für Profis: Wir vermitteln die oberen 10% Wissen. Geballtes Wissen und umfangreiche Praxiserfahrung aus erster Hand.

SUPPORT

Wir sind das Backup für Ihre Linux-Administration: LPIC-2-Profis lösen im Heinlein CompetenceCall Notfälle, auf Wunsch auch in SLAs mit 24/7-Verfügbarkeiten.

HOSTING

Wenn Hosting kein Massengeschäft sein darf: Individuelles Business-Hosting mit perfekter Maintenance durch unsere Linux-Profis. Sicherheit und Verfügbarkeit werden bei uns groß geschrieben.