

Unwissenheit schützt vor Strafe nicht...

Recht ist nicht Recht!

Die verschiedenen Rechtsbereiche.

- ▶ **Strafrecht**
 - ▶ Der Staat sichert den Rechtsfrieden, sanktioniert sozialschädliches Verhalten
 - ▶ StR wird sich nur indirekt auf das Zusammenleben der Bürger aus
- ▶ **Zivilrecht / Bürgerliches Recht**
 - ▶ Aka „Vertragsrecht“: Verhältnis zwischen Kunde und Anbieter
 - ▶ Leistung, Bezahlung, Minderung, Schadenersatz etc. etc.
- ▶ **Öffentliches Recht**
 - ▶ Verwaltungsakte und andere „hoheitliche“ Angelegenheiten
 - ▶ DatenschutzR, SteuerR, PolizeiR & Co

Wie erkennt man einen Juristen?

Das kommt drauf an...

- ▶ Ein klares „Richtig“ und „Falsch“ gibt es nicht.
- ▶ Vieles ist und bleibt Auslegungssache
 - ▶ Der Laie kann nicht „auslegen“: Er kennt weder Definitionen, noch allg. Rechtsprinzipien, noch Analogien, noch Literaturmeinungen
 - ▶ Für Auslegung ist oft Kenntnis der bislang ergangenen Rechtsprechung nötig
- ▶ Je nach Richter kann man Sachen so oder so sehen
 - ▶ Nicht umsonst werden Prozesse bis zum BGH geführt und in jeder Instanz anders entschieden

Bitte: Keine Pauschalisierungen von Einzelfallentscheidungen!

- ▶ Rechtsfragen müssen immer exakt im Einzelfall beurteilt werden
 - ▶ Bereits Kleine Änderungen in der Situation können zu entgegengesetzte Ergebnisse oder gar der Anwendung völlig anderer Rechtsvorschriften führen
- ▶ Laien übertragen gerne auf grundsätzliche (aber anders gelagerte) Situationen. => Falsche Ergebnisse!
 - ▶ Bsp: ISP hat Konkurrent mittels RBL-Blacklisting schikaniert / behindert
 - ▶ OLG Hamburg: Ist rechtwidrig: „RBL-Block kann unlauterer Wettbewerb sein“
 - ▶ Medien + Laien: „RBL-Listen **sind** als unlauterer Wettbewerb illegal“

Was dieser Vortrag leisten kann und soll

- ▶ Einen Überblick über Probleme und Fallstricke
 - ▶ Sie müssen Wissen, wo Gefahren lauern und wo Sie sich informieren müssen.
- ▶ Eine erste Einschätzung
 - ▶ Gewinnen Sie ein „Gefühl“ was wohl wie gesehen werden wird :-)
- ▶ Die Erkenntnis der Dringlichkeit
 - ▶ „Es besteht Handlungsbedarf“
- ▶ Die Erkenntnis, daß Selfmade-Jura nicht funktioniert
 - ▶ Sie brauchen kompetente (!) Rechtsberatung eines technisch verständigen (!) auf diese Themen spezialisierten (!) Juristen

Wieso darf ich dann etwas zu diesem Thema sagen?

- ▶ Diplom-Jurist – aber nicht aktiv als Jurist tätig
 - ▶ Grundsätzliche Bewertung aller Rechtsfragen und Auslegungen
 - ▶ Nicht 100%ig über aktuellste Rechtssprechung auf dem Laufenden
 - ▶ Anwesende spezialisierte Anwälte werden sich ggf. sicher aktueller auskennen
- ▶ Tägliche technische Praxis rund um Mailserver seit 1992
 - ▶ Kleine technische Details (Unterschied Bounce \Leftrightarrow Reject!) sind für die juristische Beurteilung entscheidend
 - ▶ Wer die technischen Details nicht versteht kann keine juristisch saubere Lösung entwickeln => Problem vieler Anwälte!
 - ▶ Ich berate als Techniker – stets mit dem Ziel einer juristisch sauberen Lösung
 - ▶ Wenn ich Rechtsfragen habe gehe ich zu meinem Anwalt.
Wenn der Mail-Probleme hat geht er zu mir.

Die wichtigsten Rechtsfragen im Überblick

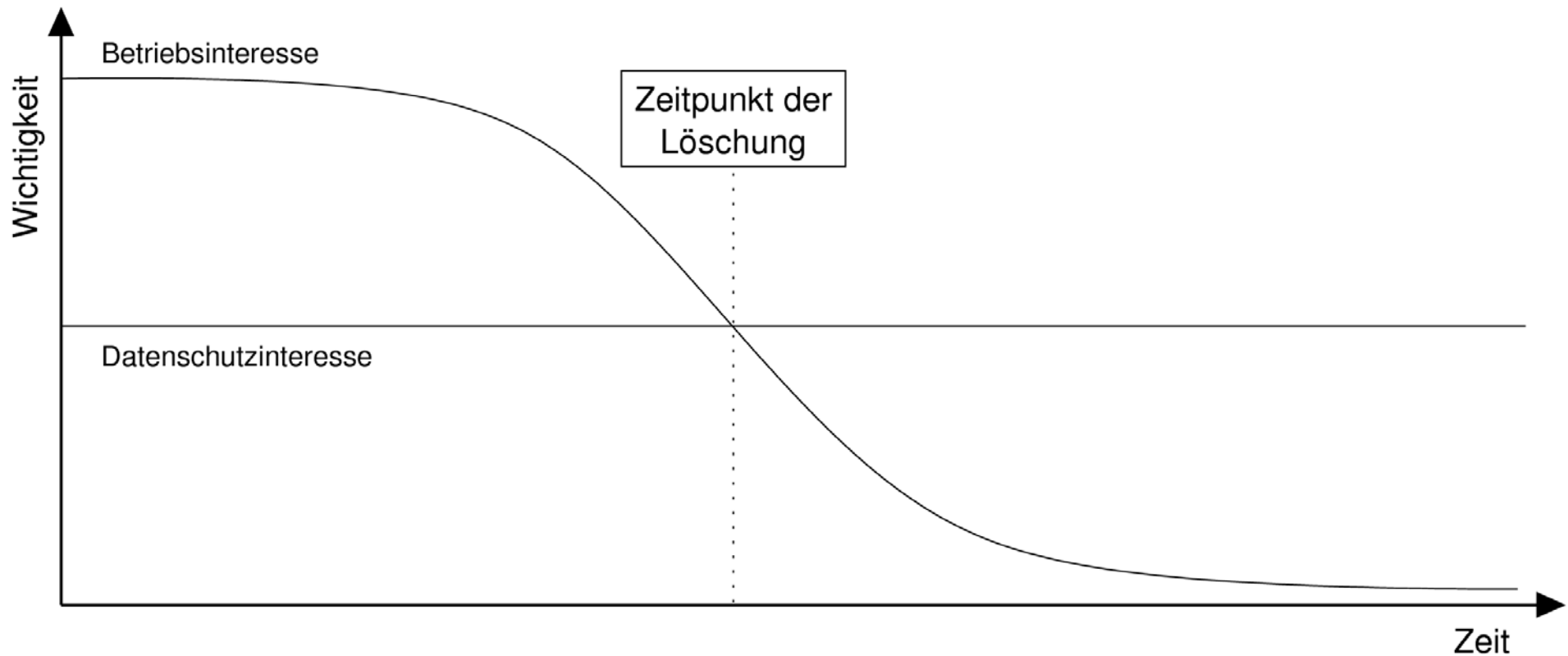
- ▶ Datenschutz und Logfiles
- ▶ Rechtsvorschriften für Unternehmen
- ▶ Private (Mail-) Nutzung am Arbeitsplatz
- ▶ Spamfilterung und ihre Fallstricke
- ▶ Zivilrechtliche Ansprüche von Absender oder Empfänger

Datenschutz und Logfiles

Kurz zusammengefaßt: Datenschutz und Logfiles

- ▶ Personenbezogene Daten dürfen grundsätzlich nicht erhoben werden.
 - ▶ Personenbezogen: Erlaubt Rückschlüsse auf konkrete Person
 - ▶ Name, Mailadresse, IP-Adresse (wenn Person bestimmbar)
 - ▶ Logfiles: Mail, Webserver, Proxy, Firewall, DHCP etc.
- ▶ „Grundsätzlich nicht erhoben“
 - ▶ Es sei denn, es ist im Einzelfall notwendig
 - ▶ Betrieb des Servers, Überwachung, Auswertung, Abrechnung...

► Zwei sich widersprechende Interessen – Abwägung!



► Es gibt keine gesetzlich definierte Frist!

Wägen Sie ab. Vorher.

- ▶ Wann ist das Betriebs- kleiner als das Datenschutzinteresse?
 - ▶ Kann je nach Umfeld unterschiedlich gewichtet werden
- ▶ Sammeln Sie Argumente: Wann müssen Sie die Daten haben?
 - ▶ Überzeugen Sie den Richter. Oder ihre Oma.
 - ▶ Wie lange ist die Queue-Haltezeit? 5 Tage.
 - ▶ Welche Zeit brauchen Userreklamationen? 3 Tage
 - ▶ Wochenende! 2 x 2 Tage!
 - ▶ Gesamt: Ca. 12-14 Tage. Nicht wesentlich mehr.

Sichern Sie sich ab: Der Persilschein.

- ▶ Fixieren Sie das schriftlich („Persilschein“)
 - ▶ Sichern Sie sich auch persönlich ab.
 - ▶ Im Team: Mit IT-Leiter, GF, Justiziar, Datenschutzbeauftragtem, Betriebsrat
 - ▶ Schriftlich fixiert mit Darlegung der Gründe und Schlußfolgerungen.
- ▶ Machen Sie es einem Richter leicht zuzustimmen.
 - ▶ Legen Sie dar, dass Sie sorgfältig (!) wohlüberlegt (!) und technisch versiert (!) abgewogen haben.
 - ▶ Kein Richter wird Ihrer ordentlich-sauberen Abwägung widersprechen solange sie im glaubwürdig-nachvollziehbaren Rahmen bleibt.
 - ▶ Der Richter wird Ihnen mit Freude folgen. Der will auch nur fertig werden.

Der Datenschutzbeauftragte: Macht der eigentlich seinen Job?

- ▶ Für die Einhaltung der Datenschutzvorschriften haftet der Datenschutzbeauftragte.
 - ▶ Der ist nicht weisungsbefugt (!) sondern „berichtet“ nur direkt Geschäftsführung
 - ▶ Eigentlich müßte der Datenschutzbeauftragte ständig nervös den Admins auf die Tastatur schauen und klare Regelungen erlassen.
 - ▶ Der Datenschutzbeauftragte ist hier also erster Ansprechpartner auf der Suche nach klaren Regeln, Abmachungen und Kontrollen.

Gar nicht speichern versus alles speichern.

- ▶ Vorratsdatenspeicherung etc. und DatenschutzG widersprechen sich.
 - ▶ Richtig. Das ist so.
 - ▶ Wie man es macht, macht man es verkehrt.
 - ▶ Verlangen Sie von mir keine klare Lösung.
- ▶ BverffG: Getrennte Datenbasis anlegen!

Rechtsvorschriften für Unternehmen

Signaturen unter geschäftlichen E-Mails

- ▶ E-Mails = Handelsbriefe
 - ▶ Pflichtangaben auf Briefpapier = Pflichtangaben auf E-Mails
 - ▶ Daten müssen originär in der E-Mail enthalten sein => Signatur
 - ▶ Keine unsichtbaren Header, keine Links auf Webseiten.
- ▶ Fast alle Unternehmen haben das umgesetzt.
 - ▶ Problem: Private E-Mails vom Arbeitsplatz werden mit Firmensignatur versandt.
 - ▶ Dürfte ein Mitarbeiter auf Firmenbriefpapier private Briefe schreiben?
 - ▶ (Wer haftet beim E-Bay-Verkauf vom Arbeitsplatz aus?)

Revisionssichere Archivierung von „Handelsbrief-Mails“

- ▶ Handelsbriefe = Alle Briefe, die die Vorbereitung, Durchführung oder Abwicklung eines Handelsgeschäfts betreffen
 - ▶ Vorbereitung: Preisliste, erstes Angebot, aber auch Infoanfrage und Auskunft!
 - ▶ Durchführung: Absprachen, Liefertermin, Änderungen
 - ▶ Abwicklung: Rechnung, Reklamationen
 - ▶ Keine Handelsbriefe: Interne E-Mails der Firma (keine Außenwirkung!).
- ▶ E-Mails = Handelsbriefe
 - ▶ Archivierungszeit für steuerlich relevante Daten: 10 Jahre
 - ▶ Archivierungszeit für alle anderen Handelsbriefe: 6 Jahre
 - ▶ Revisionssicher speichern = nicht unbemerkt veränderbar. Auch nicht von root!
 - ▶ Originär digitale Daten originär digital auswertbar speichern: Excel bleibt Excel. Kein PDF. Kein Ausdruck.

- ▶ Ganz kleiner werblicher Hinweis im eigener Sache:

Heinlein Mail-Archiv speichert als fertige Appliance revisionssicher und gesetzeskonform. Hier am Stand.

Private (Mail-) Nutzung am Arbeitsplatz

Private Nutzung: Erlaubt oder verboten?

- ▶ Oft: Schriftliches Verbot
- ▶ Aber: Entscheidend ist tatsächlich betrieblich ausgeübte Praxis
 - ▶ Keine Formvorschriften!
 - ▶ „Duldung“ kann ebenso rechtswirksame Vereinbarung sein.
 - ▶ Erlaubt oder nicht erlaubt? Was würde meine Oma sagen?
- ▶ Also: Oft durch lange wissentliche Duldung erlaubt!
 - ▶ Nutzungserlaubnis wird Bestandteil des Arbeitsvertrages!
 - ▶ Nur durch Änderungskündigung abschaffbar!
 - ▶ Firma wird plötzlich „ISP“ gegenüber Mitarbeiter. TKG anwendbar.
 - ▶ Immense (!) juristische und technische Probleme

Die Auswirkungen erlaubter privater Nutzung von E-Mails

- ▶ Was haben persönliche E-Mails im Firmenbackup zu suchen?
 - ▶ Nichts. Aber wie will man das trennen?
- ▶ Mitarbeiter will keinen Spamschutz. Er ist ja „ISP-Kunde“.
 - ▶ Firma will Spamschutz. Aber wie will man das trennen?
- ▶ Mitarbeiter wird krank: Kein Zugriff aufs Postfach!
 - ▶ Auch wenn Millionenschaden droht. Private Daten sind privat.
 - ▶ Unerlaubter Zugriff kann Verletzung der Persönlichkeitsrechte bedeuten.
- ▶ Mitarbeiter scheidet aus: Kein Zugriff auf das Postfach!
 - ▶ Ganz am Rande: Was ist mit „C:\Eigene Dokumente“?
 - ▶ Mit dem Mitarbeiter geht das Wissen der Firma.
 - ▶ Gefeuerter MA müßte zustimmen. Firma ist optimal für Abfindungen erpressbar.

Private Nutzung: Wie ist das Dilemma lösbar?

- ▶ Private Nutzung verbieten
 - ▶ Handy-E-Mail-Internet für jeden für wenige EUR verfügbar
 - ▶ Zahlreiche Freemailer für Mitarbeiter nutzbar
 - ▶ 16 Mbit-DSL für lau an jeder Ecke zu bekommen
 - ▶ Sollte Firma aus „Freundlichkeit“ den Angestellten die private Nutzung ermöglichen? Rechtsrisiko? Immenser Kosten? Erpressbarkeit?
- ▶ Oder vollständig eigene Struktur für private Nutzung aufbauen
 - ▶ Klare Trennung über Mailadresse: @privat.firma.de
 - ▶ Virenschutz Ja, Spamfilter ggf. nein (Quotas einführen?)
 - ▶ Kein Langzeit-Backup
 - ▶ Keine Signaturen
 - ▶ Ggf. nur Bedienung über Webmailer um Nutzung eher klein zu halten?

Spamfilterung und ihre Fallstricke

Die unbefugte Unterdrückung anvertrauter Nachrichten.

- ▶ § 206 StGB, Verletzung des Post- oder Fernmeldegeheimnisses
 - ▶ Mitarbeiter eines Unternehmens, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt...
 - ▶ ...der unbefugt eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt...
 - ▶ ...wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
 - ▶ (Gilt auch für Unternehmen im Umfeld oder Zulieferer.)
- ▶ Es wird keine „gewerbliche“ Erbringung gefordert!
- ▶ „Geschäftsmäßig“ ist auch die unentgeltliche private Nutzung am Arbeitsplatz.

Wann sind Nachrichten unterdrückt?

- ▶ Was ist eine „Unterdrückung“?
„Dauerhaftes oder nicht nur vorübergehendes Vorenthalten“
 - ▶ Quarantäne: Nein, solange Nutzer ohne größere Hürden an die Mails gelangt.
 - ▶ Greylisting: Nein, keine (dauerhafte/wesentliche) Unterdrückung
 - ▶ Spamordner: Nein, da Nutzer an Mails gelangt
Problem: Automatisiertes Ablöschen des Ordners nach x Tagen?
 - ▶ DISCARD: Ja.
(=Mail annehmen, aber löschen und nicht zustellen.)

Wie kann eine Befugnis eingeholt werden?

- ▶ Aber: „befugte“ Unterdrückung ist immer erlaubt!
- ▶ Geschäftliche Nutzung:
 - ▶ Geschäftliche E-Mails gehören dem „Chef“, nicht dem Mitarbeiter
 - ▶ Eigentümer kann mit seinem Eigentum machen, was er will. Auch wegwerfen.
 - ▶ Zentrale Entscheidung durch „Chef“ des Unternehmens = erteilte Befugnis
- ▶ Private Nutzung:
 - ▶ Schwierig. Nutzer müßten einzeln zustimmen.
 - ▶ Anderen juristische Meinungen reicht Zustimmung durch Betriebsrat.
- ▶ So oder so: Kein „Discard“ - kein Problem.

Dürfen E-Mails getaggt werden?

- ▶ Taggen von E-Mails (unsichtbar) im Header oder (sichtbar) im Betreff könnte Datenmanipulation i.S.d. § 303a StGB sein.
- ▶ Überwiegende juristische Meinung: Nein, solange Betreff erhalten wird und nur klar erkennbar um Tag ergänzt wird.
- ▶ Aber: Abschneiden von Attachments: Klare Manipulation und/oder sogar auch „Unterdrückung“. => Nicht machen.
 - ▶ Mail nie verändern.
 - ▶ Stattdessen: Mail rejecten oder annehmen und unverändert durchlassen.

Die Rolle des Betriebsrates

- ▶ **Kontrollfunktion des Betriebsrats!**
 - ▶ BR kontrolliert, ob kein Diskriminierungsverstoß vorliegt etc.
 - ▶ BR müßte Spamfilter-Konzept genehmigen
 - ▶ BR hat kein Mitspracherecht bezügl. Sinn & Zweck und technische Realisierung

Zivilrechtliche Ansprüche von Absender oder Empfänger

Ansprüche des Empfängers gegen seinen ISP (=Arbeitgeber)

- ▶ Wegfiltern von Spam könnte „Schlechtleistung“ des ISPs sein
 - ▶ Vielleicht will Nutzer Spam haben?!
 - ▶ Opt-In-Lösung denkbar.
- ▶ False Positive könnte „Schlechtleistung“ des ISPs sein!
 - ▶ Nutzer bezahlt ISP für Empfang.
 - ▶ Übrigens: Geschuldet ist nach BGB nur „mittlere Art und Güte“.
- ▶ Aber: Mail muß technisch i.O. und „empfangbar“ sein.
 - ▶ Auch für Briefe gelten objektiv (!) angewandte Vorschriften:
Technisch: Form, Gewicht, Briefmarke, Adressierung
Inhaltlich: Kein Sprengstoff, kein Hamster, kein...
 - ▶ Kaputte / gefälschte / RFC-widrige Mails = nicht empfangbar?

Zivilrechtliche Auswirkungen bei False Positives

- ▶ Unternehmen filtert E-Mail:
Kein §206 StGB aber ggf. Vertragsbruch ggü. Kunde.
 - ▶ Kunde bestellt unter Kaufleuten wie immer => es wird nie geliefert.
 - ▶ Wer haftet bei False Positive wenn ein Schaden entsteht?
- ▶ Tagging
 - ▶ Absender hat „250 OK“ = Einschreiben. Unternehmen hat Mail nicht ordnungsgemäß bearbeitet.
- ▶ Reject
 - ▶ Absender erhält Bounce und weiß Bescheid
 - ▶ Absender kann i.d.R. keine Schadenersatz-Forderung aufmachen
 - ▶ Ursache für Filterergebnis i.d.R. vom Absender gesetzt: „Trifft den Richtigen“
 - ▶ Selbst wenn: Vergleichbar mit technischer Störung von Fax oder Telefonanlage.

Welche Schlußfolgerungen müssen wir ziehen?

- ▶ Private Nutzung?
 - ▶ Extrem heikel und schwierig, kann Unternehmensführung eigentlich kaum verantworten.
- ▶ Archivierung von E-Mails?
 - ▶ Zwingend notwendig, kann richtig Ärger bei Betriebsprüfung geben.
- ▶ Spamfilterung?
 - ▶ Saubere Spamschutz mit Rejects ist der beste Weg und fast überall relativ problemlos machbar.
- ▶ Logfiles?
 - ▶ Fast überall Datenschutzverstöße die je nach Unternehmen ebenfalls richtig Ärger nach sich ziehen können.

Wie soll ein Administrator sicher arbeiten können?

- ▶ Selbst Juristen wissen kaum, was „richtig“ und was „falsch“ ist
 - ▶ Irgendwann bildet sich gerichtliche Rechtsprechung über Jahre hinweg.
- ▶ IT-Leiter und Administrator sind i.d.R. juristischer Laien
 - ▶ Sie sind weder dafür ausgebildet, noch dazu angestellt um selbstständig rechtssichere Lösungen finden.
 - ▶ Der Administrator benötigt juristische Vorgaben oder Unterstützung um das Unternehmen, aber auch um sich abzusichern.
 - ▶ Das Unternehmen muß ihnen qualifizierte Rechtsberatung zukommen lassen.
 - ▶ Fordern Sie das ein.
(Geschäftsführung: Fördern Sie das, der Admin handelt in Ihrem Interesse!)

Tipps zur Wahl des Anwalts

- ▶ Der Anwalt muß auf hohem Niveau E-Mails und SMTP verstanden haben. Sonst kann er nicht beraten.
 - ▶ Unterscheidung BOUNCE <=> REJECT?
 - ▶ Unterscheidung SMTP-Envelope und Mailheader?
 - ▶ Ab wann ist eine E-Mail tatsächlich angenommen?
 - ▶ Was ist ein Reverse Lookup im DNS?
 - ▶ Wie funktioniert Greylisting, SpamAssassin, policyd-weight und RBL?
- ▶ Fragen Sie Ihren Anwalt.
 - ▶ Suchen Sie sich einen Bastler mit eigenem Rootserver oder einen alten Haudegen mit Akkustikkoppler und C64/Atari/Amiga.

Wenn es um echtes Papier geht:

▶ Das Postfix-Buch

Sichere Mailserver mit Postfix

- ▶ Der Klassiker mit rund 750 Seiten in 3. Auflage
- ▶ Auch juristische Inhalte beleuchtet



▶ „POP3 und IMAP“

Mailserver mit Courier und Cyrus

- ▶ Erläutert auch Detailwissen über IMAP und Mailstorage
- ▶ Courier sehr einfach auf Dovecot übertragbar, Prinzipien und nötiges Wissen sind identisch



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.

Ja, diese Folien stehen als PDF im Netz...

<http://www.heinlein-support.de>

Soweit, sogut.

Fragen?

(Für detaillierte filligrane Rechtsdiskussion werden wir leider kaum Zeit haben...)

Und nun...

- ▶ **Vielen Dank für's Zuhören...**
- ▶ **Schönen Tag noch...**
- ▶ **Und viel Spaß an der Tastatur.**
- ▶ **Bis bald.**



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.