Peer Heinlein <p.heinlein@heinlein-support.de>

Unwissenheit schützt vor Strafe nicht...

Peer Heinlein <p.heinlein@heinlein-support.de>

Geht's um E-Mail....

- Peer Heinlein
  - Linux Security Consultant seit 1995
  - Spezialist für Mailserver und Anti-Spam/Anti-Virus
  - Diplom-Jurist / Prädikatsexamen
  - Kunden:
    - ISPs > 100.000 Kunden (EWEtel, Strato)
    - Universitäten, Forschungseinrichtungen
    - diverse Landesrechenzentren (ITDZ, Stuttgart, Baden-Franken, Thüringen)
    - Div. politische Instititionen und Stiftungen
    - Spezialfälle >> n-Millionen Mails/Tag (XING, StudiVZ)
  - Heinlein Support GmbH: 17 Mitarbeiter mit Sitz in Berlin

Peer Heinlein <p.heinlein@heinlein-support.de>

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

Peer Heinlein <p.heinlein@heinlein-support.de>

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 Rechtssprechung 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

Peer Heinlein <p.heinlein@heinlein-support.de>

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 Lüneburg: Ist rechtwidrig: „RBL-Block kann unlauterer Wettbewerb sein“
  - Medien + Laien: „RBL-Listen **sind** als unlauterer Wettbewerb illegal“

Peer Heinlein <p.heinlein@heinlein-support.de>

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

Peer Heinlein <p.heinlein@heinlein-support.de>

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 <=> 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.

Peer Heinlein <p.heinlein@heinlein-support.de>

Die wichtigsten Rechtsfragen im Überblick

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

Peer Heinlein <p.heinlein@heinlein-support.de>

Datenschutz und Logfiles

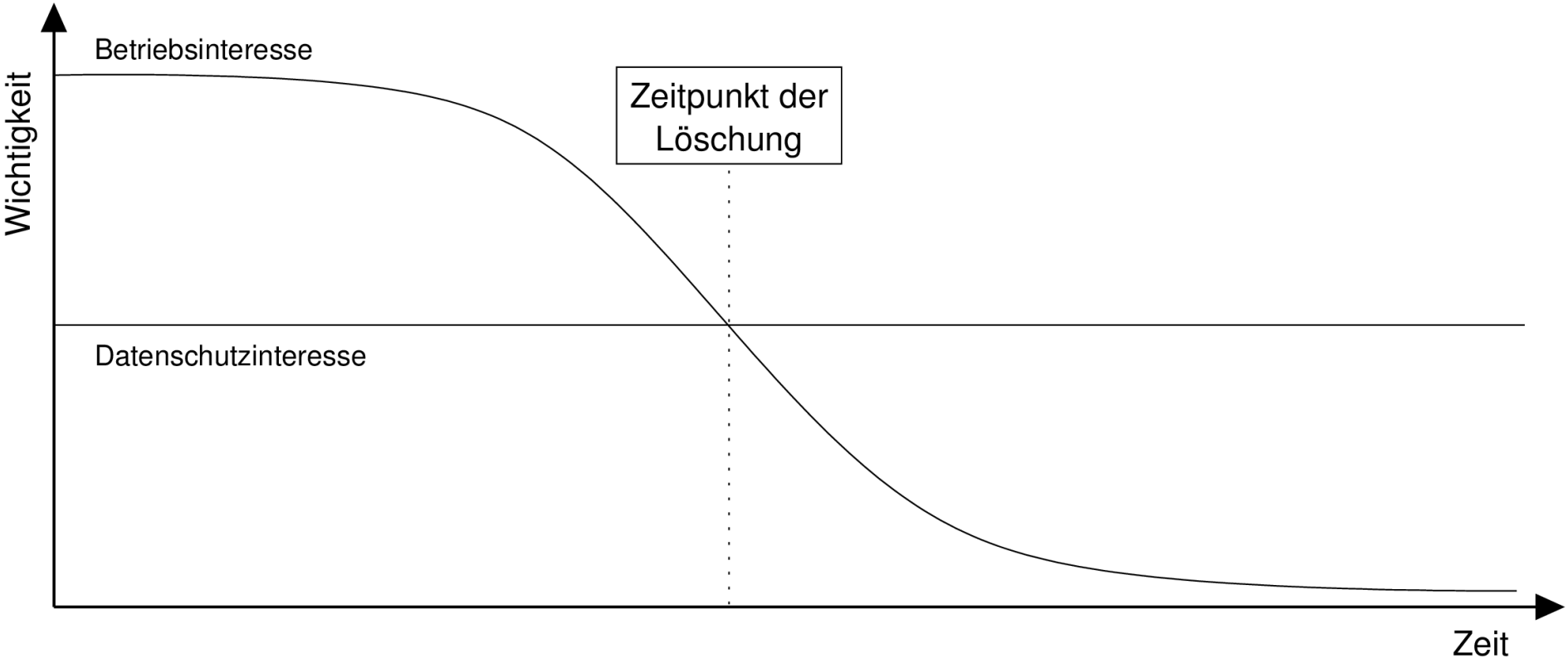
Peer Heinlein <p.heinlein@heinlein-support.de>

Kurz zusammengefaßt: Datenschutz und Logfiles

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

Peer Heinlein <p.heinlein@heinlein-support.de>

- Zwei sich widersprechende Interessen – Abwägung!



- Es gibt keine gesetzlich definierte Frist!

Peer Heinlein <p.heinlein@heinlein-support.de>

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.

Peer Heinlein <p.heinlein@heinlein-support.de>

Sichern Sie sich ab: Der Persilschein.

- Fixieren Sie das schriftlich („Persilschein“)
  - Sichern Sie sich auch persönlich ab.
  - Im Team: Mit IT-Leiter, GF, Justiziar, Datenschutzbeauftragte, 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.

Peer Heinlein <p.heinlein@heinlein-support.de>

Der Datenschutzbeauftrage: 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.

Peer Heinlein <p.heinlein@heinlein-support.de>

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!

Peer Heinlein <p.heinlein@heinlein-support.de>

Rechtsvorschriften für Unternehmen

Peer Heinlein <p.heinlein@heinlein-support.de>

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?)

Peer Heinlein <p.heinlein@heinlein-support.de>

Revisionssichere Archivierung von „Handelsbrief-Mails“

- Handelsbriefe = Alle Briefe, die die Vorbereitung, Durchführung oder Abwicklung eines Handelsgeschäfts betreffen
  - Vorbereitung: Preisliste, erstes Angebot, 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
  - Archivierunsgzeit für alle anderen Handelsbriefe: 6 Jahre
  - Revisionssicher = nicht unbemerkt veränderbar. Auch nicht von root!
  - Originär digitale Daten originär digital auswertbar speichern: Excel bleibt Excel. Kein PDF. Kein Ausdruck.

Peer Heinlein <p.heinlein@heinlein-support.de>

- Ganz kleiner werblicher Hinweis im eigener Sache:

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

Peer Heinlein <p.heinlein@heinlein-support.de>

Private (Mail-) Nutzung am Arbeitsplatz

Peer Heinlein <p.heinlein@heinlein-support.de>

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

Peer Heinlein <p.heinlein@heinlein-support.de>

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 für Abfindungen erpressbar.

Peer Heinlein <p.heinlein@heinlein-support.de>

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?

Peer Heinlein <p.heinlein@heinlein-support.de>

Spamfilterung und ihre Fallstricke

Peer Heinlein <p.heinlein@heinlein-support.de>

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.

Peer Heinlein <p.heinlein@heinlein-support.de>

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.)

Peer Heinlein <p.heinlein@heinlein-support.de>

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.

Peer Heinlein <p.heinlein@heinlein-support.de>

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.

Peer Heinlein <p.heinlein@heinlein-support.de>

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

Peer Heinlein <p.heinlein@heinlein-support.de>

Zivilrechte Ansprüche von Absender oder Empfänger

Peer Heinlein <p.heinlein@heinlein-support.de>

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?

Peer Heinlein <p.heinlein@heinlein-support.de>

Zivilrechtliche Auswirkungen bei False Positives

- Unternehmen filtert E-Mail: Kein §206 StGB
  - Kunde bestellt unter Kaufleuten wie immer => es wird nie geliefert.
  - Wer haftet bei False Positive wenn ein Schaden ensteht?
- 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.

Peer Heinlein <p.heinlein@heinlein-support.de>

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.

Peer Heinlein <p.heinlein@heinlein-support.de>

Wie soll ein Administrator sicher arbeiten können?

- Selbst Juristen wissen kaum, was „richtig“ und was „falsch“ ist
  - Irgendwann bildet sich gerichtliche Rechtssprechung 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!)

Peer Heinlein <p.heinlein@heinlein-support.de>

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.

Peer Heinlein <p.heinlein@heinlein-support.de>

Heinlein Support ist der Ansprechpartner bei allen Mailfragen

- Schulungen und Hands-On-Workshops
- Spam- und Virenfilter Inhouse / Hosted
- E-Mail-Archivierung
- E-Mail-Verschlüsselung
- Rechtssichere Umsetzung privater Mailnutzung am Arbeitsplatz
- Mailcluster > 250.000 Nutzer
- Massenversand > 1 Million Empfänger
- Groupwarelösungen unter Linux

- Natürlich und gerne stehe ich Ihnen jederzeit mit Rat und Tat zur Verfügung und freue mich auf neue Kontakte.

Peer Heinlein

Mail: p.heinlein@heinlein-support.de

Telefon: 030/40 50 51 - 42

- Wenn's brennt:
  - Heinlein Support 24/7 Notfall-Hotline: 030/40 505 - 110

heinlein

Peer Heinlein <p.heinlein@heinlein-support.de>

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

http://www.heinlein-support.de/vortrag

Peer Heinlein <p.heinlein@heinlein-support.de>

Soweit, so gut.

Gleich sind Sie am Zug:
Fragen und Diskussionen!

Peer Heinlein <p.heinlein@heinlein-support.de>

Und nun...

- Vielen Dank für's Zuhören...
- Schönen Tag noch...
- Und viel Erfolg an der Tastatur...

Bis bald.

heinlein

Peer Heinlein <p.heinlein@heinlein-support.de>

Heinlein Support hilft bei allen Fragen rund um Linux-Server

HEINLEIN AKADEMIE

Von Profis für Profis: Wir vermitteln in Training und Schulung die oberen 10% Wissen: geballtes Wissen und umfangreiche Praxiserfahrung.

HEINLEIN HOSTING

Individuelles Business-Hosting mit perfekter Maintenance durch unsere Profis. Sicherheit und Verfügbarkeit stehen an erster Stelle.

HEINLEIN CONSULTING

Das Backup für Ihre Linux-Administration: LPIC-2-Profis lösen im CompetenceCall Notfälle, auch in SLAs mit 24/7-Verfügbarkeit.

HEINLEIN ELEMENTS

Hard- und Software-Appliances für Archivierung, IMAP und Anti-Spam und speziell für den Serverbetrieb konzipierte Software rund ums Thema E-Mail.