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

Die Pflicht zur revisionssicheren E-Mail-Archivierung

- Peer Heinlein
  - Linux Security Consultant seit 1995
  - Spezialist für Mailserver und Anti-Spam/Anti-Virus
  - Kunden:
    - ISPs > 100.000 Kunden (EWEtel, Strato), Universitäten
    - diverse Landesrechenzentren (ITDZ, Stuttgart, Baden-Franken, Thüringen)
    - T-Systems Enterprises (IVBB)
    - Spezialfälle >> n-Millionen Mails/Tag (XING, StudiVZ)
  - Diplom-Jurist
  - Heinlein Support GmbH: > 20 Mitarbeiter mit Sitz in Berlin

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

Die rechtlichen Vorschriften im Schnelldurchlauf

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

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

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

Handels- und Geschäftsbriefe

- Briefe zwischen Geschäftspartnern (auch zu Privatperson!)
  - Jedes "Schriftstück" (auch E-Mail) zur
    - Vorbereitung
    - Abschluss
    - Durchführung
    - oder Rückabwicklung

    eines Geschäftes dient.
- Beispiele
  - Bestellung & Rechnung
  - Aber auch: Infoanfrage, Angebot, Katalogbestellung
  - Aber auch: Liefertermine, Absprachen, Reklamationen, Versandanzeigen
- Verweis in §147 Abs. 1 Nr. 2 AO: Archivierung gefordert

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

Firmeninterner Schriftverkehr

- Firmeninterner Schriftverkehr (zwischen Mitarbeitern) ist kein Geschäfts- oder Handelsbrief.
- Keine Archivierung!
  - (Ausnahmen in Konzern-Konstrukten möglich!)

Grundsätze ordnungsgemäßer DV-gestützter Speicherbuchführung (GoBS)

- Auch aus den Anforderungen an eine ordnungsgemäße Buchführung ergeben sich bereits Archivierungspflichten
- Die Grundsätze sind laut GoBS:
  - Vollständigkeit (!)
  - Ordnung
  - Sicherheit
  - Unveränderlichkeit (!)

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

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

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

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.
- Verstöße könnten steuerrechtliche Straftatbestände auslösen (§ 370 AO, § 378 AO, §283b StGB)

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

Die strafrechtliche Bedeutung

- § 283b StGB Verletzung der Buchführungspflicht
  - (1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer

    1. Handelsbücher, zu deren Führung er gesetzlich verpflichtet ist, zu führen unterlässt oder so führt oder verändert, dass die Übersicht über seinen Vermögensstand erschwert wird,

    2. Handelsbücher oder sonstige Unterlagen, zu deren Aufbewahrung er nach Handelsrecht verpflichtet ist, vor Ablauf der gesetzlichen Aufbewahrungsfristen beiseite schafft, verheimlicht, zerstört oder beschädigt und dadurch die Übersicht über seinen Vermögensstand erschwert,

    3. entgegen dem Handelsrecht

       a) Bilanzen so aufstellt, dass die Übersicht über seinen Vermögensstand erschwert wird, oder

       b) es unterlässt, die Bilanz seines Vermögens oder das Inventar in der vorgeschriebenen Zeit aufzustellen.

  - (2) Wer in den Fällen des Absatzes 1 Nr. 1 oder 3 fahrlässig handelt, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

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

Auswirkungen für Unternehmer und Geschäftsführer

- Verletzung von Buchführungspflichten sind Verletzungen von Kardinalpflichten eines Geschäftsführers
- Dies kann Folgen bis hin zur Haftung des GF aus privatem Vermögen nach sich ziehen („Geschäftsführerhaftung“)

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

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)

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

Sonderfall:
Die öffentlich-rechtliche Hand

Rechtsstaatsgebot, Art. 20 III GG

- Nirgendwo Archivierungspflicht wie bei Unternehmen gefordert
- Aber: Rechtsstaatlichkeit der Verwaltung, Art. 20 III GG
  - Ordentliche Aktenführung hat Verfassungsrang!
- Beweiswert von E-Mails nach VwGO? Stark eingeschränkt!
  - Fehlende ordnungsgemäße Aktenführung kann zur Beweislastumkehr führen!

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

Privatrechtliche Tätigkeiten der öffentlich-rechtlichen Hand

- Beteiligung an privatrechtlichen Unternehmen möglich
  - Steuerrechtliche Behandlung wie ein Privater!
- Problem: Abgrenzung Zweck- / gewerblicher Geschäftsbetrieb
  - Dokumentation und Nachvollziehbarkeit helfen!

Auskünfte, Akteneinsicht, Informationsfreiheitsgesetz

- Dezentrale unstrukturierte Aktenführung darf Recht auf Akteneinsicht nicht unterlaufen
  - Pflicht zur ordnungsgemäßen Aktenführung
- Behörde muß wissen, wo was gespeichert wird
  - Problem bei Wildwuchs „auf dem Desktop“

Aufsichtsbehörden und ihr Recht auf Akteneinsicht

- Kommunen werden durch Aufsichtsbehörden kontrolliert
- Dienst- und Fachaufsicht
- Rechungsprüfungsbehörden

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

Zusammengefaßt: Archivierungspflichten der öffentlich-rechtlichen Hand

- Ist prinzipiell nicht von HGB, GmbHG, AktienG, AO etc. erfaßt.
- Rechtsstaatlicher Gesetzesvollzug
  - Erfordert umfangreiche Dokumentation => Eingang der E-Mails in Akte?
- Wirtschaftliche Geschäftsbetriebe
  - 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

Im Ergebnis...

- Egal welche Rechtsgrundlage:

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

  - Auch Auswirkungen auf öffentlich-rechtliche Hand!

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

Die revisionssichere Archivierung

Wie darf/muss gespeichert werden?

- Originäres elektronische Daten müssen weiterhin elektronisch archiviert werden (§147 Abs. 5 + GDPdU!)
  - 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)

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

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!

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

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

Archivierungskonzepte im Vergleich

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

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

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

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!

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

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?

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

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!

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

Die Probleme in der Praxis

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

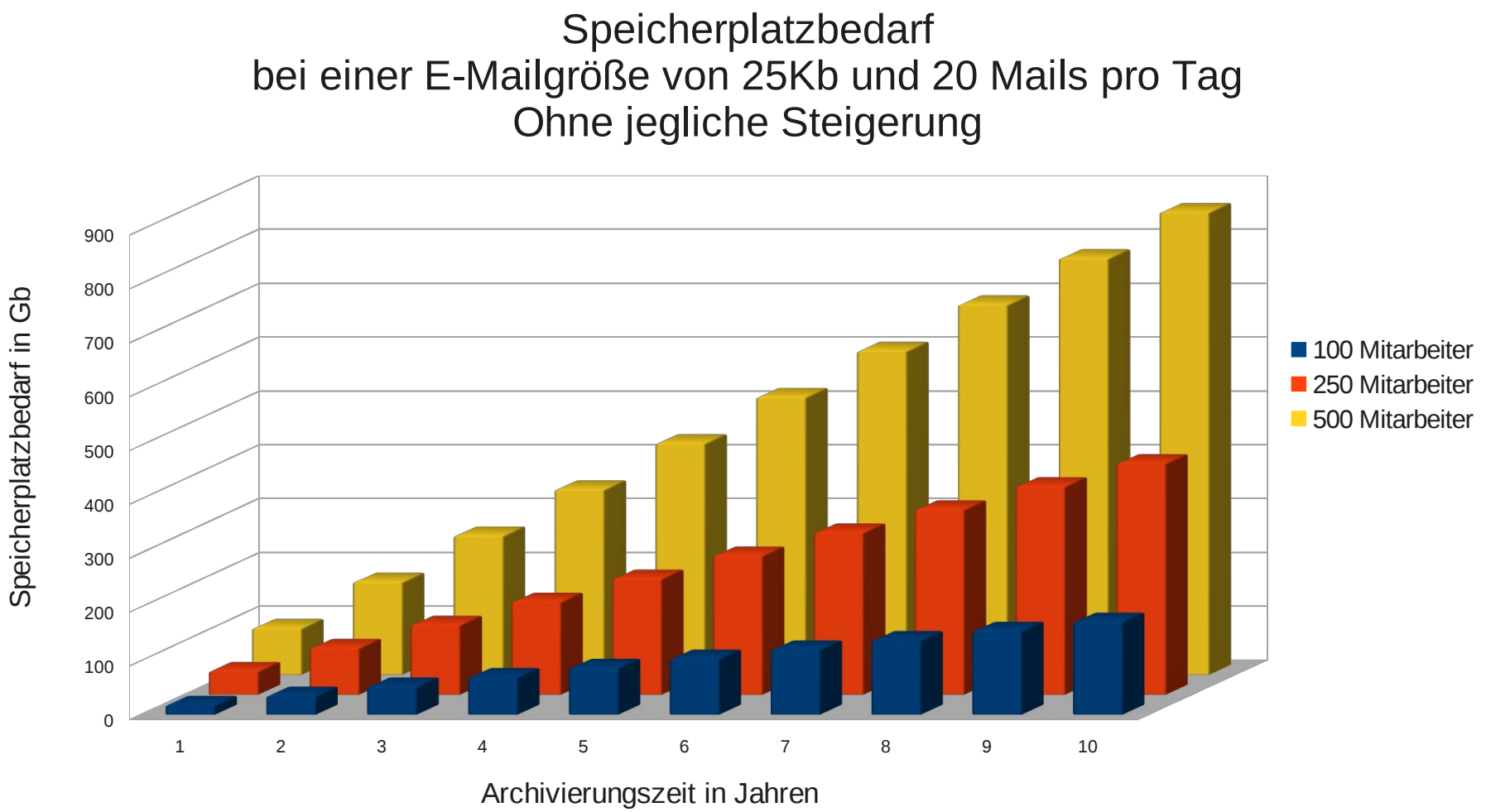
Revisionssicherheit: Ich bin root, ich kann alles?

- 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

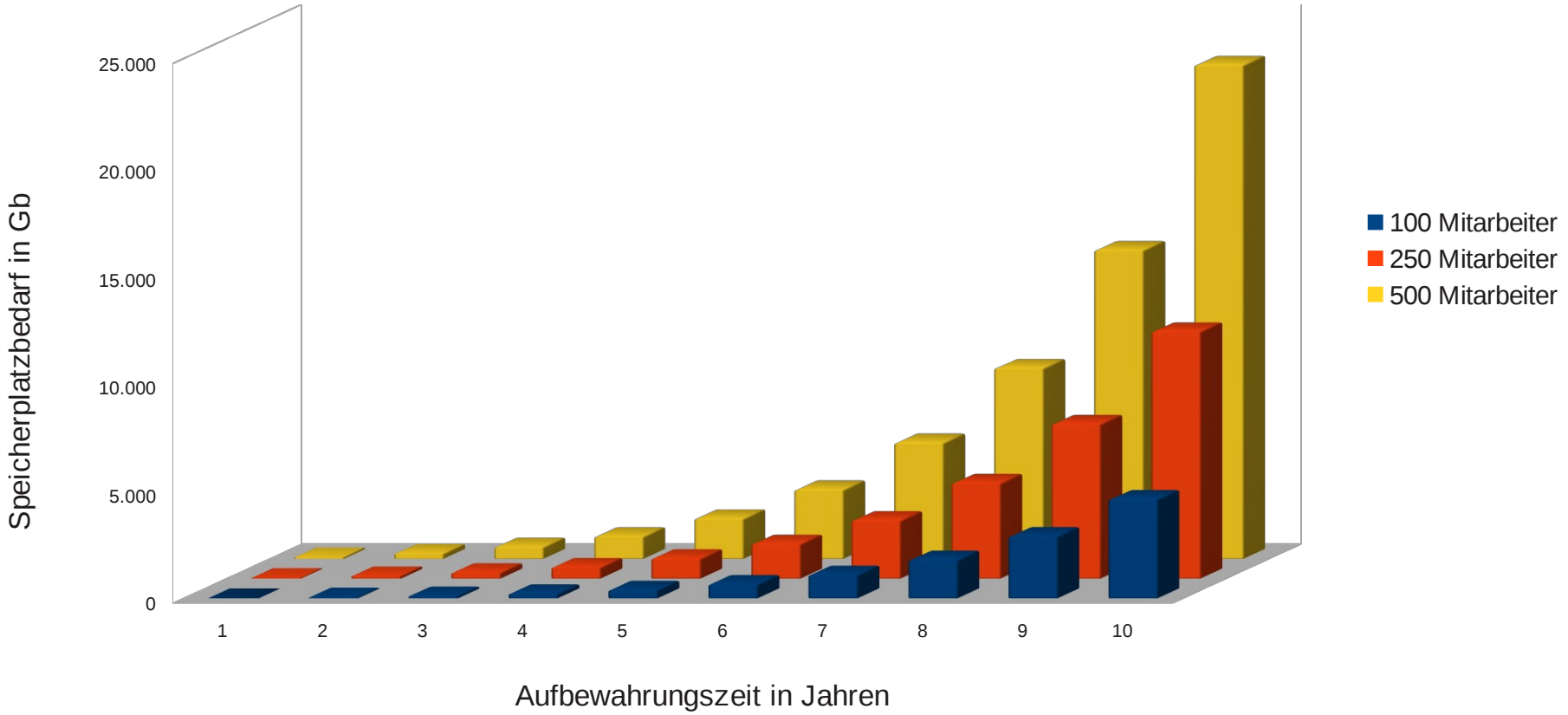
Anforderung an die Kryptographie der Revisionssicherheit

- 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.

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



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



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

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!)

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?!

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

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...

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.

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

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.

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

Es sei uns erlaubt anzumerken...

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

Heinlein Elements: Mail-Archiv

- Aus Kundenprojekten heraus entstanden
  - Heute: gesetzeskonforme, revissionssicheren und interoperable Lösung
- 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!

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!

Und nun...

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

Bis bald.

heinlein

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.