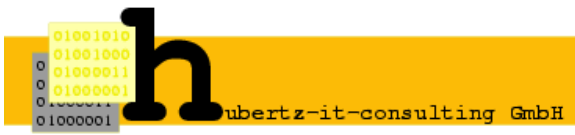
Email – im Geschäft nicht ohne Risiko

— FrOSCon 2009 —

Johannes Hubertz

hubertz-it-consulting GmbH

St. Augustin, 23. August 2009



Gliederung

- Vorstellung
- Einführung ins Thema
- Email: rechtlicher Rahmen
- Email: technischer Rahmen
- Netzwerk: Standort und Technik
- Netzwerk: Zugriffe, wer darf was wiederfinden?
- Speicherung: Medien, Orte, Cryptokram
- Ausblick: Es gibt viel zu tun ...

Vorstellung: Johannes Hubertz

1980 Hardware-Reparatur: Ersatzteile auf Bauteilebene

1987 Erstkontakt mit Unix (SCO-Xenix) und C

1994 Erstkontakt mit IP

1996 Xlink, root@www.bundestag.de, ...

1997 SSLeay, ipfwadm mit shell-scripts

1998 „Ins Allerheiligste“, iX 1/1998, Heise Verlag

2001 Gibraltar, FreeSwan, iptables ...

2001 Firmenteilung $\rightarrow$ Entwicklung und Betrieb `sspe`

2002 Weiterentwicklung und Betrieb von `sspe`

seit 1973 Bundesanstalt Technisches Hilfswerk in Köln-Porz

seit 2001 Segeln, am liebsten auf Salzwasser

Vorstellung: hubertz-it-consulting GmbH

Erkenntnisse aus dem Berufsleben

Bellovin and Cheswick: Firewalls and Internet Security, 1994

Fazit: Keep it simple!

Oder mit Einstein: So einfach wie möglich, aber nicht einfacher!

Etwas Erfahrung war Voraussetzung

Gründung am 8. August 2005, Sitz in Köln

Geschäftsinhalt: Dienstleistungen im Umfeld der IT-Sicherheit

Logo: Johannes Hubertz Certificate Authority als ASCII-7Bitmuster

Diese paar Bits findet sich in einigen 10000 X.509 Anwenderzertifikaten in der Seriennummer wieder

Wir sind käuflich ;-)

Sind das nur viele **alte** Hüte

- Email: uucp oder wie ging das noch?
- Email: smtp $\leftrightarrow$ war da sonst noch was?
- RFC 524 – 13. Jun 1973 – Proposed Mail Protocol
- RFC 733 – 21. Nov 1977 – STANDARD FOR THE FORMAT OF ARPA NETWORK TEXT MESSAGES
- RFC 822 – 13. Aug 1982 – STANDARD FOR THE FORMAT OF ARPA NETWORK TEXT MESSAGES
- RFC 1341 – Jun 1992 – MIME (Multipurpose Internet Mail Extensions)
- RFCs 1421-1424 – Feb 1993 – Privacy Enhancement for Internet Electronic Mail
- RFCs 1521-1522 – Sep 1993 – MIME (Multipurpose Internet Mail Extensions) Part 1+2
-

RFC	**wann**	**Titel**
2045	Nov.1996	MIME Part One: Format of Internet Message Bodies
2046	Nov.1996	MIME Part Two: Media Types
2047	Nov.1996	MIME Part Three: Message Header Extensions for Non-ASCII Text
2048	Nov.1996	MIME Part Four: Registration Procedures
2049	Nov.1996	MIME Part Five: Conformance Criteria and Examples

Email – mehr als Technik!

Email: Rechtlicher Rahmen

- BGB, §§ 238 ff. HGB
- GmbHG, AktG
- §§ 140 Abgabenordnung, § 14b UStG
- GDPdU (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen)
- Eigenes Interesse an ordentlicher Geschäftsführung, Haftungsminimierung

Email: Rechtlicher Rahmen II

- War das schon alles?
- Post- und Fernmeldegeheimnis (StGb)
- BDSG, Landesdatenschutzgesetze
- Keine eineindeutige Rechtsprechung
- Unterschiedliche Standpunkte
- Ansichtssache? (BVerfG: Recht auf Privatheit!)
- Konsequent: Verbot privater Nutzung des Mediums Email im Unternehmen
- Addon: Einhaltungskontrolle, Abmahnung bei Verstoss
- Ohne Kontrolle und Abmahnung kommt das reine Verbot einer Erlaubnis gleich!
- Alternativ: Einverständniserklärung **jedes** einzelnen Mitarbeiters zur Speicherung
- Keine Alternative: Betriebsvereinbarung, Privates kann nicht pauschal vereinbart sein!

Email: Nutzerverhalten I

Albert Einstein:

Um ein tadelloses Mitglied einer Schafherde zu sein,
muß man vor allem ein Schaf sein.

Emailarchiv: Was dagegen spricht

- private Nutzung
- Datenschutzgesetze
- Speicherkosten
- Überwachung unmoralisch, Betriebsvereinbarung
- Spamflut

Spam — Spassbremse im Geschäftsverkehr

- bestenfalls sinnlose Emails
- Good Times, – alt, in immer wieder neuen Varianten
- Nigeria Connection seit 1990'ern
- Werbung auf persönlicher Basis, ein gut funktionierendes Geschäftsmodell
- Schadstoffcontainer, Trojaner wird durch Endbenutzer fertig installiert
- Archivierung von Spam kontraproduktiv

Am Markt vorhandene Systeme

Werbung verspricht sich schon mal, oder?

Sie müssen alle Emails archivieren! Revisionssicher!

Ist das alles wahr?

Wo bleibt die Verhältnismäßigkeit?
Wie ist „revisionssicher“ juristisch definiert?

Marc Twain:

Man muß die Tatsachen kennen, um sie verdrehen zu können.

Archivlösungen für Compliance im Geschäft

- Nutzen nur zur Compliance fragwürdig
- Nutzen für den Endanwender schafft Mehrwert
- $\Rightarrow$ Volltextindex, Suchmöglichkeiten
- Email des Endbenutzers nicht zwingend auf seinem Arbeitsplatz
- viele kommerzielle Lösungsansätze, alle proprietär
- Hosted- oder Inhouse-Solutions
- Beispiel: ein kommerzielles Email-Archivierungssystem inhouse
- Beispiel: ein kommerzielles Email-Archivierungssystem SAAS
- keine nichtkommerziellen Lösungsansätze gefunden ausser: ArchiSafe, OpenArch, OpenBenno(neu)
- ArchiSafe: gigantisch
- OpenArch: nur eingeschränkt freie Software,
  nur die kostenpflichtige Variante ist vollständig funktional
- OpenBenno: noch nicht angesehen,
  Lizensierung ähnlich OpenArch, still ToDo!

Nutzerverhalten II

Friedrich Dürrenmatt:

Je planmässiger ein Mensch vorgeht,
desto wirksamer vermag ihn der Zufall zu treffen.

Anforderungen an eine Archivierungslösung

- Speicherung im Orginal
- Unveränderbarkeit, Nicht-Abstreitbarkeit
- Zugriffslogging
- Verschiedene Nutzerrollen: Anwender, Administrator, Betriebsprüfer
- Exportmöglichkeiten, Wiederherstellung
- Betriebssichere Funktionalität
- Keine zusätzlichen Sicherheitsprobleme im Unternehmen
- Einfache Wartbarkeit, auf Knopfdruck?

Nutzerverhalten III

Marc Twain:

Immer wenn man die Meinung der Mehrheit teilt,
ist es Zeit, sich zu besinnen ...

Begrifflichkeiten

Notwendige Voraussetzung für jede Aufbewahrung ist dauerhafte **Lesbarkeit, Integrität und Authentizität** der Dokumente. Hierzu gelten die Definitionen:

Integrität	Unversehrtheit der Daten
Authenzität	eindeutige Bestimmung der Quelle der Daten
Lesbarkeit	Sichtbarmachung[1] der in den Daten enthaltenen Informationen
Verkehrsfähigkeit	Möglichkeit, Dokumente und Akten von einem System zu einem anderen übertragen zu können, bei der die „Qualität“ des Dokuments sowie seine Integrität und Authentizität nachweisbar bleiben.
Vollständigkeit	Bezug mehrerer aufgrund eines inneren Zusammenhangs zu einer Sammlung oder auch Akte zusammengefasster Einzeldokumente ist sichergestellt.
Vertraulichkeit	Schutz vor unbefugter Kenntnisnahme zur Sicherung der Geheimhaltung personenbezogener Daten und betriebs- oder berufsbezogener Geheimnisse.

[1] Clientsoftware

Ziele – Stichwortsammlung

Administration	per cgi, perl, tainted, user www-data, root-cron macht die Arbeit Paranoia ist gefragt!
Administrator	sieht keine Emails oder Dateien. KEINE!
Backup	per cron, sql-dump, drbd, . . . , anderer Brandabschnitt!
Daten	jeweils mit Start- und Ende-Datum Ende-Datum als Lösch-Kennung Emails, Benutzer, Zertifikate, . . .
Datenbank	versch.Hashwerte, z.B. md5, sha1, ripemd160, zusammen mit den Daten
Dateien	nur einmal in DB mit Hashwerten, Eingangsdatum, Löschdatum
Ein- und Ausgangsart	Datei auf Share und / oder per Email an den Endbenutzer
Email	Attachments nur einmal in der DB Header und Body separiert abgelegt
Emaileingang	smtpd (Obtuse, debian-paket) mit zusätzl. Greylisting . . . Paranoia!
Organisations-struktur	Daten pro Benutzer verschlüsselt Vertretungs- und Nachfolgeregelung alle Änderungen loggen
Zeitstempel	Jede Einlagerung nimmt Bezug auf jeweilig letzten Zeitstempel
Zugriffsrechte	hierarchisch abgeleitet aus Organisationsstruktur Ober sticht Unter! Zwei, Vier- oder Sechsaugenprinzip für Administration

Netzwerk – sicher ohne Ausnahme

Andrew S. Grove, former CEO Intel Corp.:

Only the paranoid survive.

intern oder extern?

Was soll ins Archiv?

- von extern empfangene Emails
- nach extern gesendete Emails
- interne Emails

Alle Emails ausser die mit Viren und SPAM

Als Standort bietet sich eine DMZ an, mx auf die Archivlösung, intern ebenfalls als mailgateway für alle eingestellt.
Von aussen nur per smtp, von innen zusätzlich per https erreichbar.
Kombination mit anderen Diensten ist zu vermeiden.

Firewalltechnik ist gerade gut genug

Alt bewährt – gut erforscht – kommerziell erfolgreich:

freie Firewallsoftware: smtpd

ursprünglich für Juniper Firewalls entwickelt durch obtuse.com

- smtpd ist von Beginn an paranoid geschrieben und das ist gut so.
- smtpd ist vorgesehen als Empfänger zur Weiterleitung an einen Virenchecker
- smtpd ist hervorragend wie einfach konfigurierbar, skaliert gut
- smtpd etwas verfeinert mit greylisting, Web-Gui zur Administration,
- smtpd ist perfekt als frontend für alle Emails.
- Freie Software: `smtpd-greylist.evolvis.org` Tarent sei Dank!
- *Das Web-Gui wartet noch auf willige und fähige Entwickler . . .*

Karl Kraus:

> Satiren, die der Zensor versteht,
> werden mit Recht verboten.

Email, hier: **geschäftskritische Variante**

Greylisting Totschlagargument

Bei uns ist Email geschäftskritisch, das muss immer sofort funktionieren!

Gegenrede

Wenn jemand ernsthaft behauptet, Email sei bei Ihm geschäftskritsch,
so hat er sein Geschäft nicht verstanden!

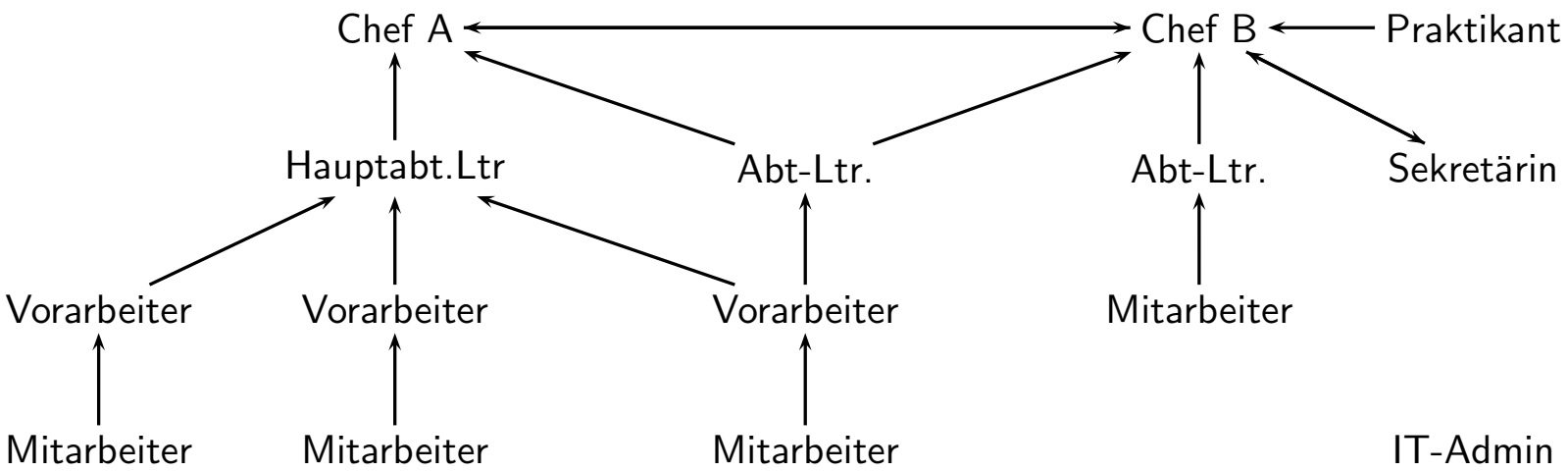
Gedenkminute

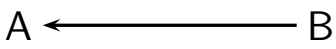
Wenn ein unbestimmt oft kaskadiertes **Queue and Forward** – System geschäftskritisch ist, dann ist das Geschäft sehr kritisch zu bewerten. Seine Geschäftsgrundlage incl. der zugrundeliegenden Mechanismen sollte man als Geschäftsmann kennen . . .

Zugriffe – streng hierarchisch mit Ausnahmen

oder wie jetzt?

Einfache Organisationshierarchie



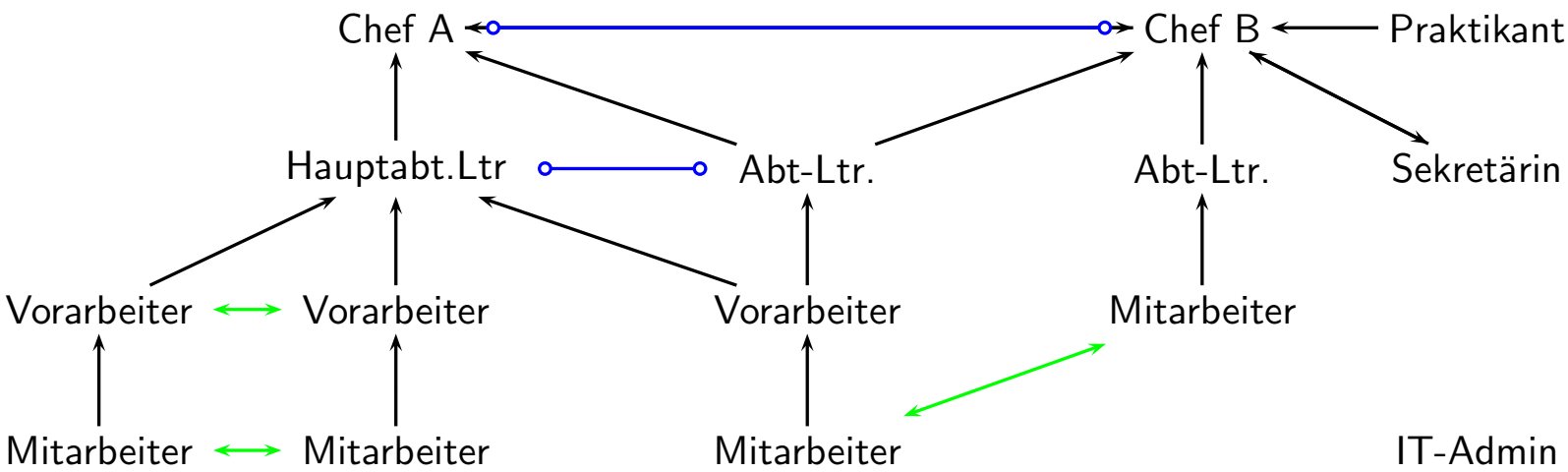


A ist Vorgesetzter von B

Wer darf nun wessen Emails lesen?

Ober sticht Unter!

Einfache Organisationshierarchie mit Vertretungen



A ← B A ist Vorgesetzter von B

A ○—○ B Gegenseitige Vertretung

A ⟷ B Urlaubsvertretung

Wer darf nun wessen Emails lesen?

Ober sticht Unter, aber variabel einstellbar!

Speicherung – wie und wo

Nutzen nur bei Verfügbarkeit

- Daten sollen durchsuchbar und benutzbar bleiben
- Bandlaufwerke, Roboterlaufwerke sind langsam und teuer
- Bandlaufwerke, Roboterlaufwerke sind schwierig im Backup
- Festplatten sind schnell und billig
- digitale Signaturen mit Zeitstempeln garantieren Unverfälschtheit
- Backup ist einfach machbar und prüfbar
- Spiegelung in anderen Brandabschnitt realisierbar
- Obere Grenze für den Aufwand: $\approx$ Schadenshöhe bei Verlust
- Untere Grenze für den Aufwand: $\sim \frac{1}{Haftungsrisiko der Geschäftsleitung}$

Erwünschte Eigenschaften

- Volumenunabhängige Suchzeiten
- Volltextsuche
- Zeitintervallbezogene Suche
- Emailattributbezogene Suche
- Kombinationen

Datenbankhaltung erstrebenswert,
Architektur unbekannt

Geforderte Eigenschaften

- Mit einer Datenbank kann die Zugriffsrechteverwaltung integriert sein
- die Datenbank kann Schlüssel für die Daten halten, Rechte liegen in Tabellen
- die Datenbank kann Suchanfragen und administrative Zugriffe (Benutzerverwaltung) loggen

Vorgaben I

1. Das Archiv enthält Emails (und manuell eingebrachte Dokumenten)
2. Emails mit erkannten Schadinhalten gelangen nicht ins Archiv
3. Benutzer-Zugriffe auf das Archiv geschehen über ein Webinterface
4. Web-Zugriffe **Z** sind durch X.509 Client-Zertifikate **U** authentisiert
5. Zu jeder Mail **M** existiert mindestens ein bekannter Absender oder ein bekannter Empfänger
6. Zu jeder Mail **M** existiert mindestens ein Empfänger **E**
7. Zu jeder Mail **M** existiert genau ein Absender **A**
8. Zu jeder Mail **M** existiert genau ein Eingangszeitpunkt **T**

Vorgaben II

1. Alle Zertifikate sind über ein Webinterface oder extern **(PKI)** verwaltet
2. Jedes Benutzer-Zertifikat ist einer oder mehreren Mailadressen (hierarch.) zugeordnet
3. Die Zertifikate bestimmen daher die erlaubten Zugriffe
4. Zertifikatseigenschaft: Benutzer **(U),** Administrator **(A)** oder Prüfer **(P)**
5. Zu jedem Benutzer können $1 \ldots n$ Vertreter **(V)** eingerichtet werden
6. Archivadministration wird geloggt, Log kann **nicht** plausibel geändert werden
7. Admin.-Zert. berechtigt **nicht** zur Benutzung des Archivs
8. Admin.-Zert. darf Prüfläufe / Plausibilitätschecks starten
9. Admin.-Zert. darf Benutzerkonten Anlegen, De- und Reaktivieren
10. Admin.-Zert. darf Vertretungsregeln Anlegen, De- und Reaktivieren
11. Admin.-Zert. (oder/mit PKI) darf Prüferkonto Anlegen und Deaktivieren
12. Admin.-Zert. darf verschlüsseltes Backup anstossen
13. Prüfer hat einen speziellen Webzugang, er definiert Suchanfragen, Admin erstellt Medium (CD, DvD) mit Ergebnissen

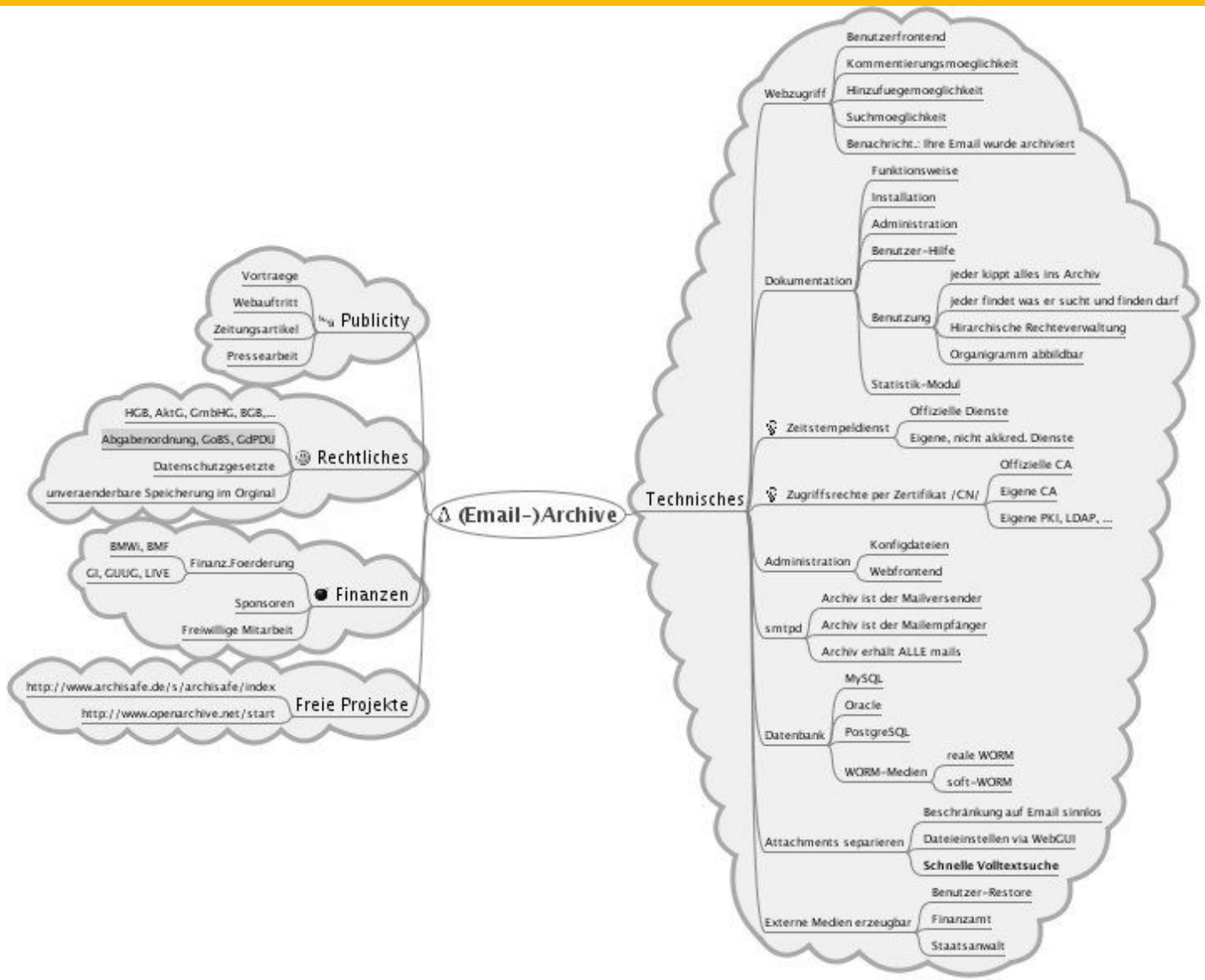
Vorgaben III

1. Das Archiv enthält regelmässig einzuholende signierte Zeitstempel
2. Zeitstempel müssen in plausibler Reihenfolge ohne Lücken auftreten
3. Zeitstempel Frequenz ist einstellbar, jedoch nur für die Zukunft
4. Toleranzen sind in festgelegten nachvollziehbaren Grenzen erlaubt
5. Toleranzgrenzen sind einstellbar, jedoch nur für die Zukunft
6. Änderung der Toleranzgrenzen erfordert Eingabe eines guten Grundes
7. Lücken führen zu Logeinträgen, mehrere aufeinander fehlende Stempel zu Stillstand
8. Triggerschwelle ist einstellbar, jedoch nur für die Zukunft
9. Stillstandseintritt wird durch Emails an def. Personenkreis unmittelbar sichtbar.
10. Wiederanlauf nur durch manuellen Eingriff des Admins (Mausklick?)
11. Wiederanlauf bedarf einer Erklärung des Administrators incl. Grund

Vorgaben IV

1. Archiv-System kann nur per ssh mit Schluessl gewartet werden
2. PKI-Zertifikate (Webserver, CA, Admin, ...) einmaliger import via ssh
3. Ohne PKI: System-Root kann CA- und Admin-Zertifkate erzeugen

es gibt viel zu tun . . .



Wer macht mit?

Quellen

RFCs: Internet, div. Fundorte

BGB, HGB, AO: Bundesanzeiger, Internet (nicht amtlich)

GoBS, GDPdU: Schreiben des BMF

Dokumentation Nr. 564 des BMWi, Rossnagel et al.

IHK-Rechtsinformation Nr. 70, IHK-Schwaben, Augsburg

`http://smtpd-greylist.evolvis.org`

`http://eneuron.evolvis.org`

Ich bedanke mich für Ihre Aufmerksamkeit

hubertz-it-consulting GmbH jederzeit zu Ihren Diensten

Ihre Sicherheit ist uns wichtig!

Frohes Schaffen

Johannes Hubertz

`it-consulting _at_ hubertz dot de`

$H\alpha \in \{$ `kompetenzspektrum.de` $\}$

powered by LaTeX 2_ε
and PSTricks