E-Mail Korrespondenz mit dem eigenen Server

Wie Hillary Clinton und Donald Trump – nur sicherer

René 'Lynx' Pfeiffer

Crowes Agency OG
https://www.crowes.eu/, rene@crowes.eu

Linuxwochen Eisenstadt
FH Burgenland, Eisenstadt, Österreich.

Table of Contents I

Table of Contents II

E-Mail Korrespondenz

Kurze Geschichte

- MITs Compatible Time-Sharing System (CTSS) (1961/1965)
- ARPANET mail (1969)
- Unix `mail` Programm (1971)
- `mail` vernetzt via Unix-to-Unix Copy (UUCP) (1978)
- BerkNet, X.400, BITNET, MCI Mail, FidoNet, . . .
- Simple Mail Transfer Protocol (SMTP), RFC 821 (1982)
- Extended SMTP (ESMTP), RFC 1869/5321 (1995/2008)
- Post Office Protocol (POP) 1/2/3, RFC 918/937/1081 (1984/1985,1988)
- Internet Message Access Protocol (IMAP), Xerox, (?)
- Internet Message Access Protocol v2/v3, RFC 1064/1176/1203 (1988/1991)
- Internet Message Access Protocol v4, IETF (>1991)

Electronic Mail (E-Mail)

- E-Mail entspricht zu 100% dem Briefverkehr
  - Umschlag = E-Mail-Kopf / Header
  - Brief = E-Mail / Body
  - Briefkasten = eingehender Server
  - Briefkasten = ausgehender Server
  - Postfach = Mailbox, Inbox
- (E)SMTP ist Store and Forward Protokoll
- ursprünglich textbasiert, mittlerweile binäre Anhänge möglich

E-Mail-Server

- E-Mail-Server hat (viele) Komponenten
- reichlich Auswahl bei der Implementation
- Hauptanforderung ist Ein-/Ausgabe
  - **Store** and Foward
  - Indizierung
  - temporäre Daten
- Hauptanforderung ist Computing
  - Filtersysteme

Warum eigener E-Mail-Server?

- E-Mail ist das letzte herstellerunabhängige Nachrichtenformat!
- E-Mail sind Geschäftskorrespondenz, Instant Messenge(r/s) nicht
- Outsourcing heißt: Dritte lesen mit
  - Werber erstellen Profile nach Inhalten
  - Filtersysteme & Backups
  - Lesezugriff nicht protokolliert
- Safe Harbo(u)r / Privacy Shield fragwürdig
- Einhaltung von Verträgen
- Schutz von Kunden
- *„Ich habe nichts zu verbergen.“* ist Kündigungsgrund für Sysadmins!

Table of Contents I

Table of Contents II

Elektrischer Briefverkehr - Komponenten

Wichtige Vokabeln

- Mail User Agent (MUA) - E-Mail Client; `mutt`, Thunderbird, . . .
- Mail Transport Agent (MTA) - E-Mail Server, primär für SMTP
- *outbound MTA* transportiert E-Mails vom Client zu Server(n)
- *inbound MTA* nimmt E-Mails von Fremden entgegen
- Relay - MTA, der E-Mails von einem MUA akzeptiert
- Local Delivery Agent (LDA) - nimmt E-Mails von MTA und legt sie in Mailbox(en)
- Unsolicited Bulk Email (UBE) / Unsolicited Commercial Email (UCE) - Spam

Was passiert wenn ein Brief angenommen wird?

1. Authentisierung Absender
2. Annahme Brief, optional Prüfung des Inhalts
3. Suche nach zuständigen Servern via Domain Name System (DNS/DNSSEC)
4. Übergabe Brief, (optional) Prüfung des Absenders, Empfängers, Inhalts und Transportwegs
5. (interne) Suche nach Postfach
6. Speicherung in Postfach
7. Authentisierung Empfänger
8. Übergabe Brief zur Ansicht

Was passiert wenn ein Brief angenommen wird? (2)

1. Authentisierung/Authentisierung Absender
2. Annahme/Annahme Brief, optional Prüfung des Inhalts
3. Suche nach zuständigen Servern via Domain Name System (DNS/DNSSEC)
4. Übergabe/Übergabe Brief, (optional) Prüfung des Absenders, Empfängers, Inhalts und Transportwegs
5. (interne) Suche nach Postfach
6. Speicherung in Postfach
7. Authentisierung/Authentisierung Empfänger
8. Übergabe/Übergabe Brief zur Ansicht

Authentisierung Absender

- Port 25/TCP ist nur für Server $\longleftrightarrow$ Server Kommunikation
- Port 587/TCP ist für Client (Sender) $\longrightarrow$ Server Kommunikation
- Client müssen sich vor Absenden einloggen oder autorisiert sein
- Authentisierung? Autorisierung?
  - Login + Passwort
  - X.509 Zertifikat
  - Whiteliste (IP Adresse)

Bezug zu DNS

- DNS Mail Exchanger (MX) Records geben Empfangsserver an
  - mehrere möglich
  - MX Priorität gibt Reihenfolge an
- MX Records sind immer Namen
- MX Server müssen immer im DNS auflösbar sein
- Forward und Reverse Lookup existieren und sind gleich
  - `mx.example.net` $\longrightarrow$ `172.23.23.1`
  - `172.23.23.1` $\longrightarrow$ `mx.example.net`

Sender Policy Framework (SPF)

- Konzept existiert seit 2000, ab 2005 umgesetzt, 2014 *proposed standard* RFC 7208
- SPF gibt legitime Quellen für E-Mails an
  - Policy wird per DNS TXT Record publiziert
  - 8 Mechanismen (ALL, A, IP4, IP6, MX, PTR, EXISTS, Include)
  - 4 Ergebnisse (*PASS*, *NEUTRAL*, *SOFTFAIL*, *FAIL*)
- sinnvoll möglichst streng zu setzen
- verwandt mit Sender ID

Sender Policy Framework (SPF) - Beispiele

```
v=spf1 a:mx.bmi.gv.at a:pv-smtp.bmi.gv.at -all
v=spf1 mx ip4:8.44.101.8/32 ip4:8.44.101.9/32 ~all
v=spf1 mx ip4:109.239.101.43 -all
v=spf1 mx a:mail1a.cia.gov a:mail1b.cia.gov a:mail2a.cia.gov
       a:mail2b.cia.gov mx:cia.gov mx:ucia.gov ~all
v=spf1 +mx ip4:153.31.0.0/16 -all
v=spf1 include:spf_a.navy.mil include:spf_b.navy.mil
       include:_spf.eemsg.mail.mil ~all
v=spf1 include:spf.protection.outlook.com -all
v=spf1 mx include:fd.dep.no ~all
v=spf1 ip4:194.18.169.43 ip4:194.18.169.45 -all
```

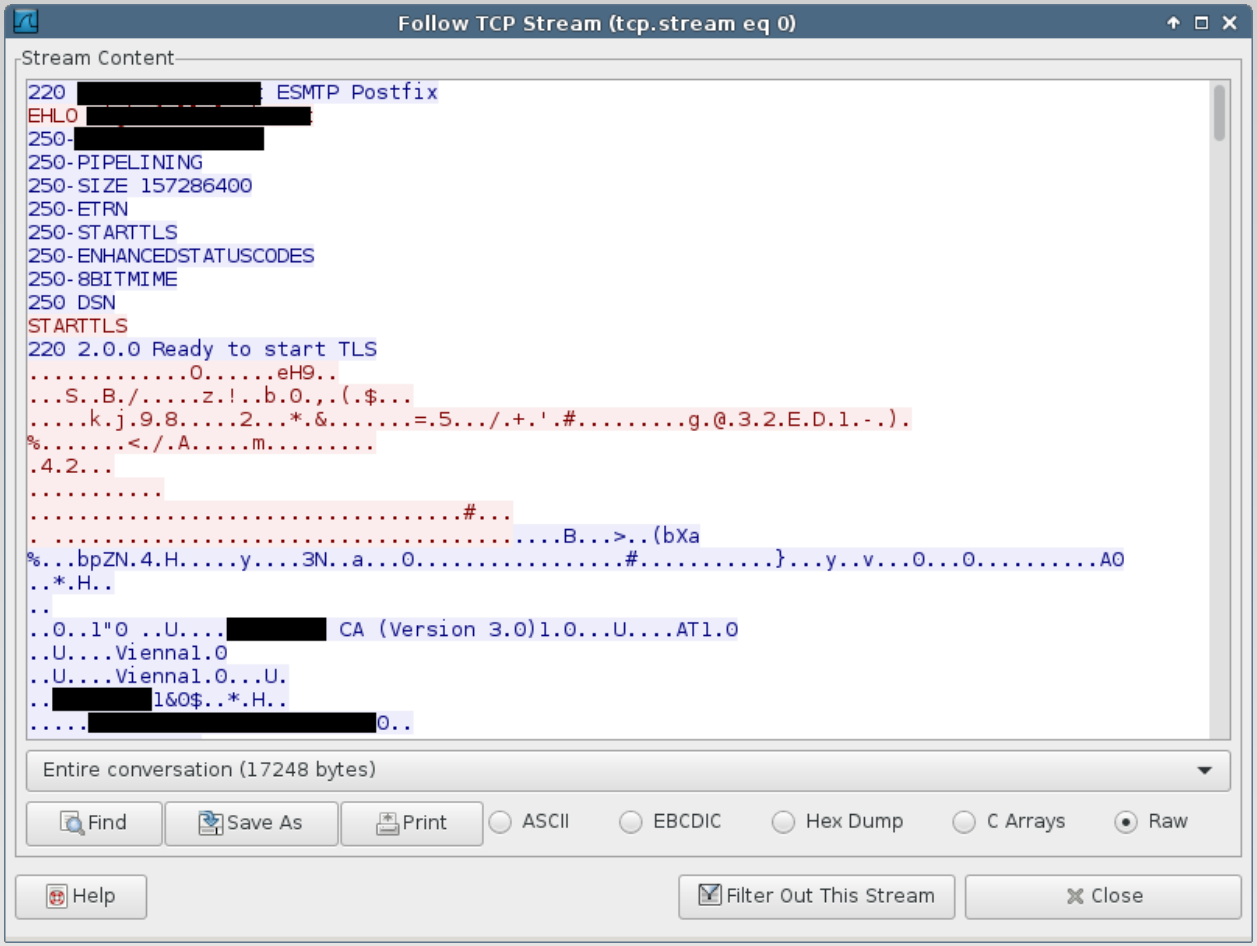
DomainKeys Identified Mail (DKIM)

- *enhanced DomainKeys* (Yahoo!) + *Identified Internet Mail* (Cisco) = DKIM
- signiert und verifiziert E-Mails Inhalte (Body)
- RFC 6376 sieht Schlüssel zwischen 512 und 2048 Bit Länge vor
- implementiert durch Proxies (Filter)
  - erfordert Kontrolle der Quelle(n)
  - PKI / Schlüsselmanagement
- Authentisierung $\neq$ Vermeidung von Mißbrauch

Verschlüsselung

- Protokolle waren ursprünglich ausschließlich Klartext
- Nachrüstung von Verschlüsselung (STARTTLS)
  - ESMTP/SMTP (25/TCP und 587/TCP) schaltet auf TLS nach STARTTLS um
  - IMAPv4 (143/TCP) schaltet auf TLS nach STARTTLS um
  - POP3 (110/TCP) schaltet auf TLS nach STARTTLS um
- TLS gleich zu Anfang (analog HTTPS)
  - SMTPS (465/TCP)
  - IMAPS (993/TCP)
  - POP3S (995/TCP)
- TLS Infrastruktur (X.509 Zertifikate & Schlüssel)

STARTTLS Nachteil



Filtersysteme und Prüfungen

- (E)SMTP Greylisting - Verzögerungen für neue Server
- Realtime Blacklist (RBL)
  - Listet auffällige Server nach Kriterien
  - 326 aktive Blacklists (laut multirbl.valli.org)
- Ruf der Quelle (Sender Reputation)
- verbotene/erlaubte Formate & Inhalte
- Antivirus Filter
- UBE/UCE Filter

Filter lassen sich beliebig kombinieren - hängt stark von Richtlinien ab.
Whitelisting besser als Blacklisting.

Realtime Blacklist (RBL)

- Vielzahl an Kriterien
  - Protokollimplementation (RFCs, Richtlinien, . . .)
  - infizierte Server oder Client, die darüber senden
  - UBE/UCE Quellen
  - verhaltensoriginelles Management
- RBL Delisting schwierig/unmöglich
- RBLs werden oft gemischt - pro RBL ein DNS Query
- RBL können verschwinden - im Auge behalten

Senderbase.org (Beispiel)

Details

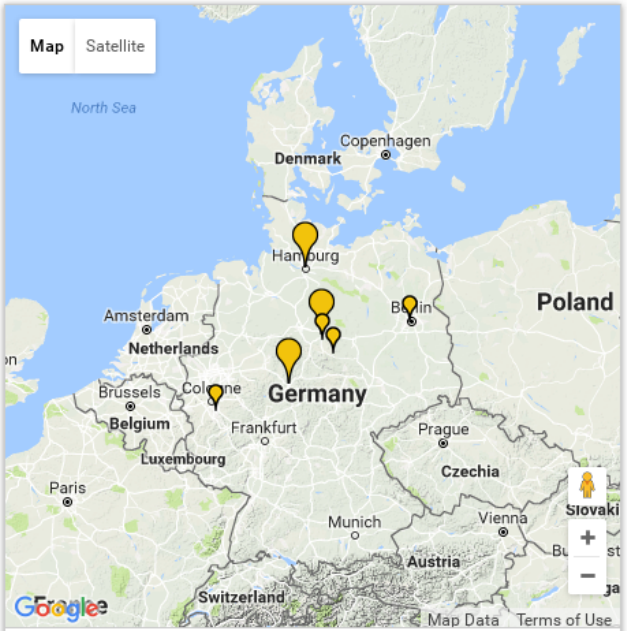
Domain	**bund.de**	
Hostname	bund.de	
Web Reputation	**Neutral**	
Web Category	Government and Law	
	Last Day	Last Month
Email Volume	4.3	4.3
Volume Change	0.1% ↑	
Mail Servers	mx1.bund.de mx2.bund.de	

Top Network Owners

1 - 3 out of 3

Network Owner	Last Month Volume ↓
Bundesamt fuer Sicherheit in der Informationstechn	4.3
Johann Heinrich von Thuenen-Institut (vTI)	2.8
Verein zur Foerderung eines Deutschen Forschungsne	1.9

Location Data



Top Cities
Germany, NULL
Germany, Hamburg
Germany, Braunschweig
Germany, Berlin
Germany, Bonn

Senderbase.org (Beispiel)

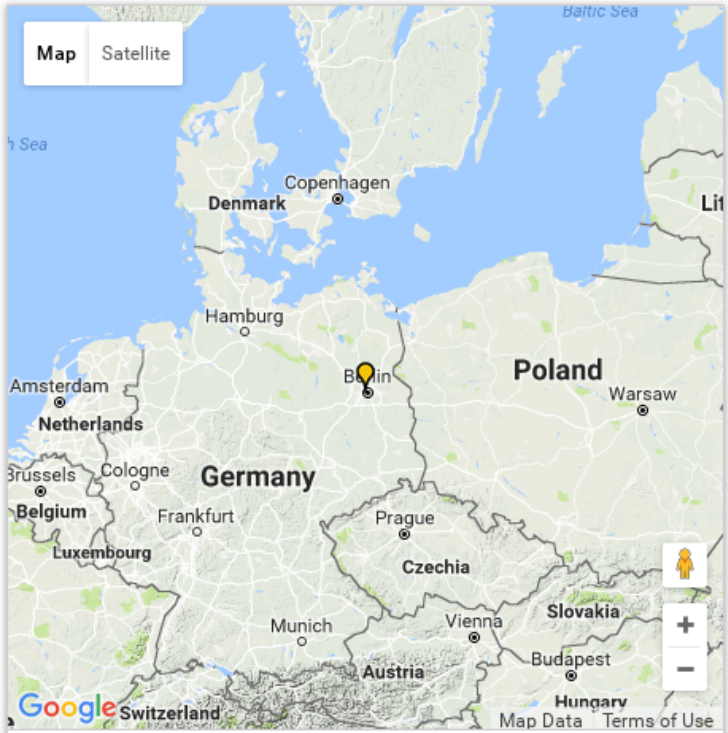
Details

Hostname	**mx1.bund.de**
Web Reputation	**Neutral**
Web Category	Government and Law

	Last Day	Last Month
Email Volume	0.0	0.0
Volume Change	0%	

Domain	bund.de
Network Owner	Bundesamt fuer Sicherheit in der Informationstechn

Location Data



City

Germany, Berlin

Formate & Inhalte (Beispiel)

```
$banned_filename_re = new_RE(
  # block certain double extensions anywhere in the base name
  qr'\.[^./]*\.(exe|vbs|pif|scr|bat|cmd|com|cpl|dll)\.?$'i,
  qr'\{[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}\}?'i, # Windows Class ID CLSID, strict
  qr'^application/x-msdownload$'i,                     # block these MIME types
  qr'^application/x-msdos-program$'i,
  qr'^application/hta$'i,
# qr'^application/x-msmetafile$'i, # Windows Metafile MIME type
  qr'^\.wmf$', # Windows Metafile file(1) type
# qr'^message/partial$'i, qr'^message/external-body$'i, # rfc2046 MIME types
# [ qr'^\.(Z|gz|bz2)$'            => 0 ],  # allow any in Unix-compressed
# [ qr'^\.(rpm|cpio|tar)$'        => 0 ],  # allow any in Unix-type archives
# [ qr'^\.(zip|rar|arc|arj|zoo)$'=> 0 ],  # allow any within such archives
  qr'.\.(ade|adp|app|bas|bat|chm|cmd|com|cpl|crt|emf|exe|fxp|grp|hlp|hta|
␣␣␣␣␣␣␣␣␣inf|ins|isp|js|jse|lnk|mda|mdb|mde|mdw|mdt|mdz|msc|msi|msp|mst|
␣␣␣␣␣␣␣␣␣ops|pcd|pif|prg|reg|scr|sct|shb|shs|vb|vbe|vbs|
␣␣␣␣␣␣␣␣␣wmf|wsc|wsf|wsh)$'ix,  # banned ext - long
  qr'.\.(doc|xls|docx|xlsx)$'ix,
# qr'.\.(mim|b64|bhx|hqx|xxe|uu|uue)$'i,  # banned extension - WinZip vulnerab.
  qr'^\.(exe-ms)$',                       # banned file(1) types
# qr'^\.(exe|lha|tnef|cab|dll)$',         # banned file(1) types
);
```

Table of Contents I

Table of Contents II

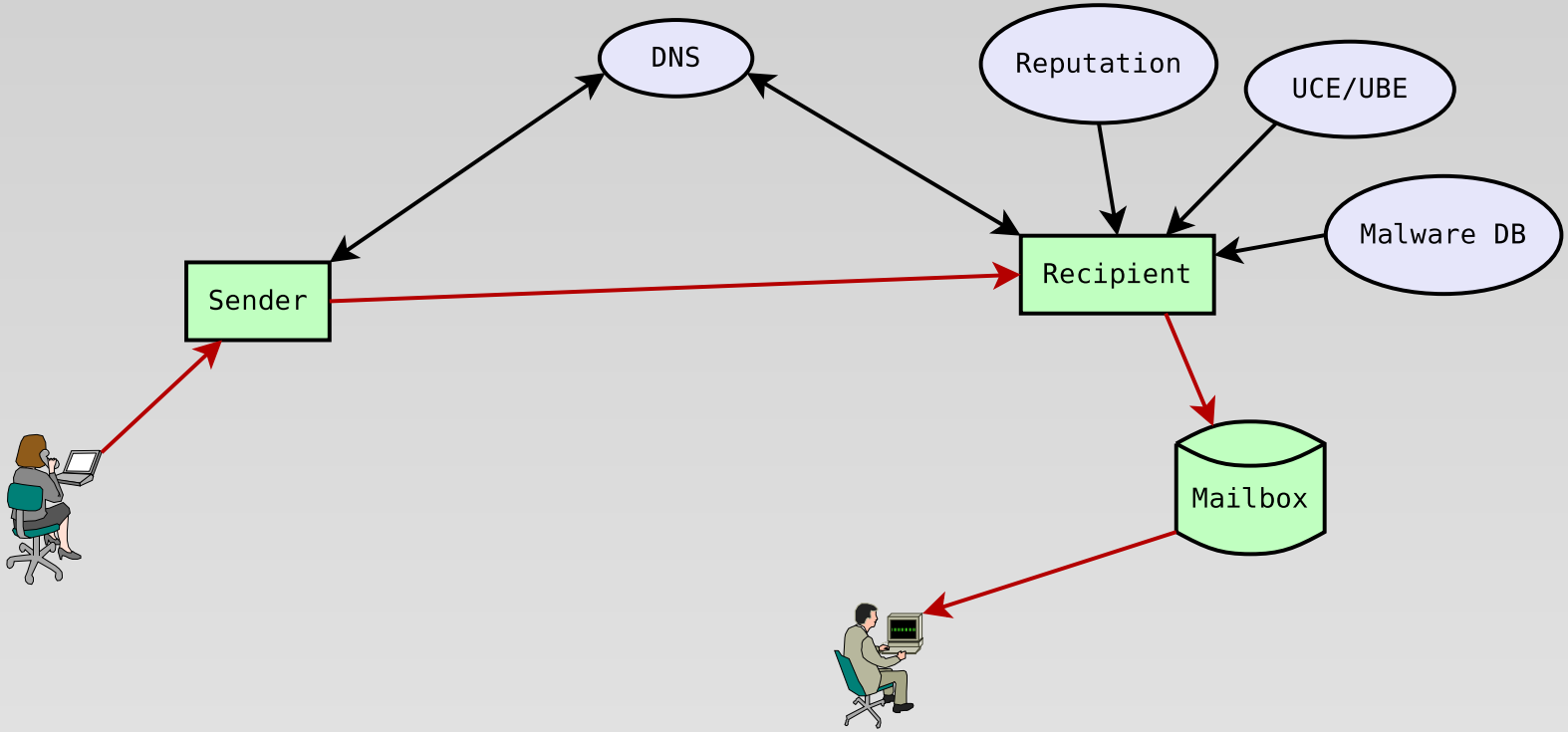
Werkzeuge


Stamp Pad Ink
Encre a Tampons
Tinta de Sellar
Stempelfarbe
LACO
OFFICE PRODUCTS
LACO
30 ml
AIR MAIL
ENTWURF
ZUR INFORMATION

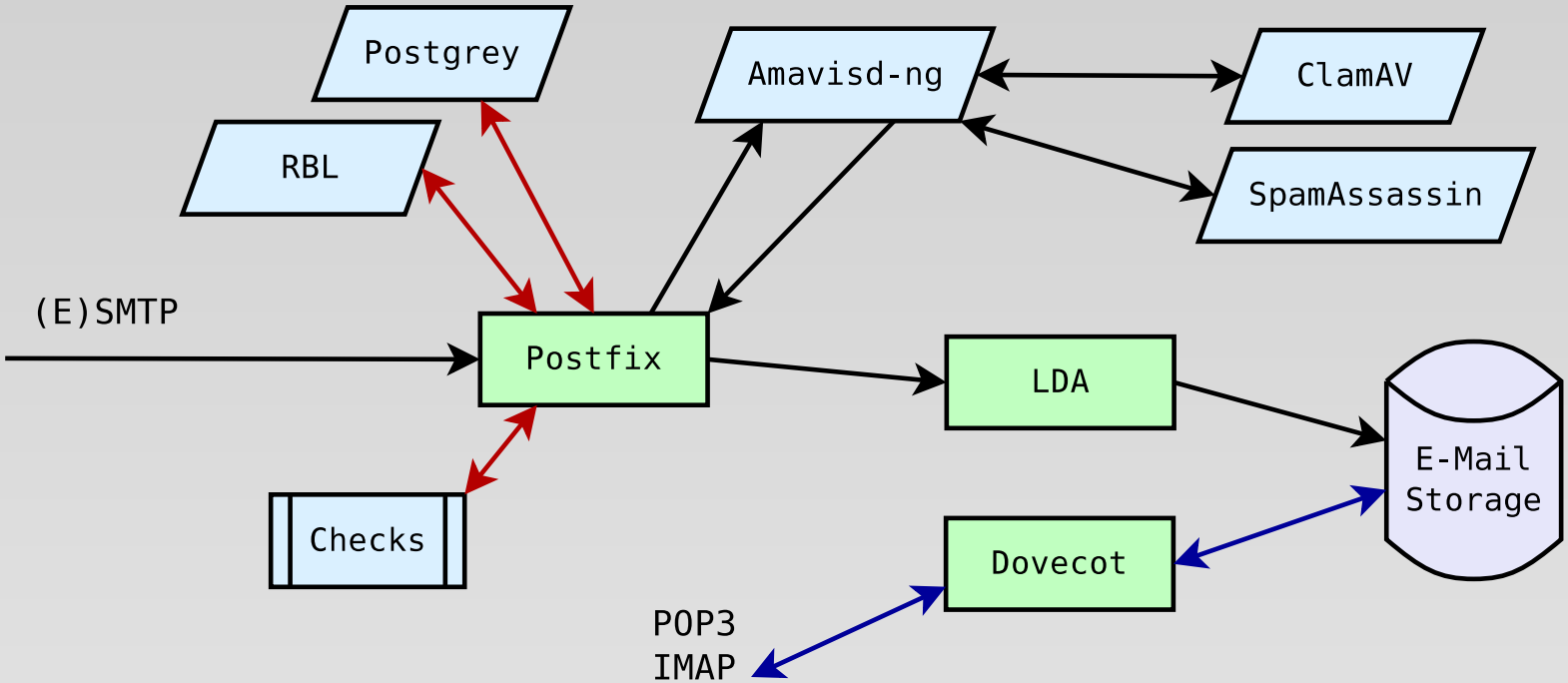
Freie Software

- Postfix (MTA) - sehr vielseitig
- Postgrey für Greylisting
- Dovecot
  - IMAP/IMAPS, POP3/POP3S
  - LMTP (LDA)
  - Simple Authentication and Security Layer (SASL)
  - Filter/Plugins möglich
- amavisd-new
  - benötigt zusätzliche Decoder für Dateiformate
  - Vielzahl von Antivirus-/Antispamfilter möglich
- SpamAssassin™ / DSPAM
- Postfix Admin als Frontend (benötigt Datenbank)

Implementation (1)



Implementation (2)



Installation

- Basissystem (Debian/Devuan bevorzugt)
- Datenbank mit Postfix Admin Schemas (MySQL/MariaDB)
- Postfix mit
  - Postgrey/amavisd-new
  - SQL Maps
  - Anti-Relay-/Content-Checks
- Dovecot mit
  - IMAP/IMAPS,
  - Maildir Storage für Mailboxen
  - SQL User Database Anbindung
- ClamAV™ Antivirusfilter

Konfigurationsdateien

- /etc/postfix/main.cf & /etc/postfix/master.cf
- /etc/postfix/{dh_512.pem,dh_2048.pem} + TLS Zertifikate / Schlüssel
- /etc/postfix/{mysql_virtual_alias_maps.cf,mysql_virtual_domains_maps.cf,mysql_virtual_mailbox_maps.cf}
- /etc/postfix/{access.sender,helo,rcpt_blacklist}
- /etc/amavis/conf.d/
- /etc/dovecot/dovecot.conf
- /etc/dovecot/sql.conf
- /etc/dovecot/conf.d/10-mail.conf
- /etc/dovecot/conf.d/10-master.conf
- /etc/dovecot/conf.d/10-ssl.conf
- /etc/dovecot/conf.d/15-mailboxes.conf

Table of Contents I

Table of Contents II

Zusammenfassung

- E-Mail Infrastruktur hat viele Komponenten.
- Eigenes Hosting läßt sich sehr genau abstimmen.
- Transportweg von Korrespondenz schwer abzusichern.
- Vortrag gibt nur Einstieg, denn
  - DNSSEC, DANE, . . .
  - UBE/UCE Abwehr im Detail,
  - PGP/GPG, S/MIME, . . . fehlen
- Konfigurationsdateien und Ansible Playbook verfügbar:
  https://github.com/rpfeiffer/mailtoaster.git

Table of Contents I

Table of Contents II

Fragen?


egid:0/0, parent /usr/
rnel: [466.100239] PAX: execution
rnel: [466.100243] PAX: terminating task: /usr/
rnel: [466.100245] PAX: bytes at PC: c3 00 00 00 00 00 00 00 0000000000400c90
rnel: [466.100256] PAX: bytes at SP-8: 0000000000400c90 0000000000400c58
038a81700870 000003da23831c38 0000000100000000
ernel: [466.100265] grsec: bruteforce prevention initiated for the next 30 minutes or until service
he crash report for /usr/lib/paxtest/execheap[execheap:4190] uid/euid:0/0 gid/egid:0/0, parent /usr/lib/paxtest
kernel: [466.100276] grsec: more alerts, logging disabled for 10 seconds
kernel: [466.100914] PAX: execution attempt in: <stack>, 39f1b2b8000-39f1b2da000 3fffffdd000
kernel: [466.100916] PAX: terminating task: /usr/lib/paxtest/execstack(execstack):4193, uid/euid: 0/0, PC: 00
kernel: [466.100918] PAX: bytes at PC: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
kernel: [466.100927] PAX: bytes at SP-8: 0000000000400b79 0000000000000000 0000000000000000
0000000000000 0000000000000000 0000000000000000
kernel: [466.101767] PAX: execution attempt in: /usr/lib/paxtest/shlibtest2.so, 3810d9a5000-3810d9a7000
kernel: [466.101770] PAX: terminating task: /usr/lib/paxtest/shlibbss(shlibbss):4196, uid/euid: 0/0, PC:
kernel: [466.101771] PAX: bytes at PC: c3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
kernel: [466.101780] PAX: bytes at SP-8: 000003810ddc7538 0000000000400eef 0000000000400c9a
0000000000400c67 000003ca56a0e5e0 000003810cf62700 0000000000000000
ey kernel: [466.102654] PAX: execution attempt in: /usr/lib/paxtest/shlibtest2.so, 31f4606e000-31f46070000
ey kernel: [466.102658] PAX: terminating task: /usr/lib/paxtest/shlibdata(shlibdata):4199, uid/euid: 0/0, PC:
rey kernel: [466.102660] PAX: bytes at PC: c3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
rey kernel: [466.102669] PAX: bytes at SP-8: 0000031f46490538 0000000000400eef 0000000000400c9a
0000000000400c67 000003844224a720 0000031f455f5700 0000000000000000
rey kernel: [466.103783] PAX: execution attempt in: <anonymous mapping>, 3a7da6f0000-3a7da6f1000
rey kernel: [466.103787] PAX: terminating task: /usr/lib/paxtest/mprotanon(mprotanon):4202, uid/euid: 0/0,
466.103790] PAX: bytes at PC: c3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PAX: bytes at SP-8: 0000000000400a6a 0000000000400c70 0000000000000000
0000000100000000
/usr/lib/paxtest/mprotbss, 00601000-00602000
/mprotbss(mprotbss):4205, uid/euid: 0/0,

Table of Contents I

Table of Contents II

Über die Crowes Agency OG

Die Crowes Agency OG ist eine Gruppe von Experten aus verschiedenen Feldern. Wir bieten unsere Erfahrungen im Rahmen von großen und kleinen Projekten an. Der Fokus liegt auf den Gebieten Grafikdesign, Software-Entwicklung, öffentlichen Erscheinungen (wie beispielsweise Webseiten und Kommunikation mit der „Außenwelt“), Systemadministration, IT Sicherheit und Unternehmensberatung. Die Crowes Agency stellt aus ihrem Pool von Mitarbeitern Teams für die Lösung von Kundenproblemen zusammen.

Kontakt Crowes Agency OG

- ℹ`https://www.crowes.eu/`
- Kontaktinformation des Autors
  - ✉`rene@crowes.eu`
  - PGP/GPG `0x28CAC51F8C413583`
  - +43.676.5626390 (Signal verfügbar)
  - +43.677.61356623 (unverschlüsselte Sprache & Signal verfügbar)
  - Threema ID `T6SB8WP6`
- E-Mail allgemeine Anfragen ✉`enquiry@crowes.eu`