Absichern eines Mailsystems

1 Einleitung

Für die zweite Abgabe im Fach Cyber Sicherheit soll ein sicherer Mail-Server und ein DNS-Server im Labor eingerichtet werden. In diesem Bericht werden die einzelnen Schritte erklärt. Anhand von relevanten Logs und einem Testmail wird gezeigt, dass die Infrastruktur wie gedacht funktioniert. Im Anhang befinden sich die wichtigsten Konfigurationsdateien in ihrem finalen Zustand.

2 DNS-Server

Die Idee ist, eine Subdomäne in der Domäne cyberlab.fhnw.ch zu definieren. Dazu müssen zuvor einige Informationen gesammelt werden. Zu Beginn werden die Nameserver der Domäne gesucht.

```
> dig cyberlab.fhnw.ch ns

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> cyberlab.fhnw.ch ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14958
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;cyberlab.fhnw.ch.              IN      NS

;; ANSWER SECTION:
cyberlab.fhnw.ch.       4774    IN      NS      srvNS02.cyberlab.fhnw.ch.
cyberlab.fhnw.ch.       4774    IN      NS      srvNS01.cyberlab.fhnw.ch.

;; ADDITIONAL SECTION:
srvNS01.cyberlab.fhnw.ch. 4774  IN      A       192.168.64.10
srvNS01.cyberlab.fhnw.ch. 4774  IN      AAAA    2001:470:b78e:8000::10
srvNS02.cyberlab.fhnw.ch. 4774  IN      AAAA    2001:470:b78e:8000::11
srvNS02.cyberlab.fhnw.ch. 4774  IN      A       192.168.64.11

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Jun 01 07:29:49 UTC 2024
;; MSG SIZE  rcvd: 177
```

Gearbeitet wurde an der Station 10, daher wurde die Subdomäne u10.cyberlab.fhnw.ch gewählt. Nun muss noch sichergestellt werden, dass NS Einträge für diese Subdomäne im Nameserver von cyberlab.fhnw.ch existieren.

```
> dig u10.cyberlab.fhnw.ch @192.168.64.10 ns +norecurse

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> u10.cyberlab.fhnw.ch @192.168.64.10 ns
+norecurse
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46369
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 04d64f2da491433101000000662f44c579f5e89e5ad9adb2 (good)
;; QUESTION SECTION:
;u10.cyberlab.fhnw.ch.                IN      NS

;; AUTHORITY SECTION:
u10.cyberlab.fhnw.ch.        4800    IN      NS      ns1.u10.cyberlab.fhnw.ch.
u10.cyberlab.fhnw.ch.        4800    IN      NS      ns2.u10.cyberlab.fhnw.ch.

;; ADDITIONAL SECTION:
ns2.u10.cyberlab.fhnw.ch. 4800    IN      A       192.168.97.81
ns1.u10.cyberlab.fhnw.ch. 4800    IN      A       192.168.97.80

;; Query time: 0 msec
;; SERVER: 192.168.64.10#53(192.168.64.10) (UDP)
;; WHEN: Mon Apr 29 06:57:09 UTC 2024
;; MSG SIZE  rcvd: 145
```

Mit diesen Informationen kann nun der DNS-Server für die Subdomäne aufgesetzt werden. Eine virtuelle Maschine wurde eingerichtet und der Dienst Bind9 darauf installiert. Diese Maschine wird ab sofort Ubuntu-DNS genannt. Ein weitere virtuelle Maschine mit Bind9 wurde zusätzlich als Ubuntu-Slave zur Verfügung gestellt.

Beide Nameserver von cyberlab.fhnw.ch werden in die Datei /etc/bind/named.conf.options auf dem Ubuntu-DNS-Server aufgenommen, um Anfragen an den DNS-Server von cyberlab weiterzuleiten, falls der lokale DNS-Server die angefragte Domäne nicht selbst auflösen kann.

```
forwarders {
        192.168.64.10;
        192.168.64.11;
 };
```

Die Konfigurationsdatei für die Zone wird unter /etc/bind/db.u10.cyberlab.fhnw.ch erstellt. Es ist wichtig sicherzustellen, dass die korrekten IP-Adressen den Nameservern zugewiesen werden. Die IP-Adressen wurden zuvor mit dem Tool dig ermittelt.

```
$TTL 10800 ; 3 Stunden in Sekunden
u10.cyberlab.fhnw.ch. IN SOA ns1.u10.cyberlab.fhnw.ch. hostmaster.u10.cyberlab.fhnw.ch. (
                                1         ; Serial
                                10800 ; Refresh after 3 hours
                                3600   ; Retry after 1 hour
                                604800         ; Expire after 1 week
                                3600   ; Negativ caching TTL of 1
)

; Nameserver
u10.cyberlab.fhnw.ch.       IN      NS      ns1.u10.cyberlab.fhnw.ch.
u10.cyberlab.fhnw.ch.       IN      NS      ns2.u10.cyberlab.fhnw.ch.

; Mailserver
u10.cyberlab.fhnw.ch.       IN      MX      10 mail.u10.cyberlab.fhnw.ch.

; Hosts
ns1.u10.cyberlab.fhnw.ch.  IN      A       192.168.97.80
ns2.u10.cyberlab.fhnw.ch.  IN      A       192.168.97.81
mail.u10.cyberlab.fhnw.ch. IN      A       192.168.97.189
```

Die Konfigurationsdatei für die Rückwärtszonen unter /etc/bind/db.192.168.97 sieht wie folgt aus. Ein Reverse-DNS-Lookup ermöglicht es, die IP-Adresse einer Maschine in ihren zugehörigen Hostnamen umzuwandeln.

```
$TTL 10800 ; 3 Stunden in Sekunden
97.168.192.in-addr.arpa. IN SOA ns1.u10.cyberlab.fhnw.ch. hostmaster.u10.cyberlab.fhnw.ch. (
                                1         ; Serial
                                10800 ; Refresh after 3 hours
                                3600   ; Retry after 1 hour
                                604800         ; Expire after 1 week
                                3600   ; Negativ caching TTL of 1
)

; Nameserver
97.168.192.in-addr.arpa.    IN      NS      ns1.u10.cyberlab.fhnw.ch.
97.168.192.in-addr.arpa.    IN      NS      ns2.u10.cyberlab.fhnw.ch.

; Reverse-Lookup
80.97.168.192.in-addr.arpa.IN      PTR     ns1.u10.cyberlab.fhnw.ch.
81.97.168.192.in-addr.arpa.IN      PTR     ns2.u10.cyberlab.fhnw.ch.
189.97.168.192.in-addr.arpa.       IN      PTR     mail.u10.cyberlab.fhnw.ch.
```

Der Bind9 Dienst muss nun noch wissen, wo die Zonendateien gespeichert sind. Bei der Ubuntu-DNS Machine definiert die Datei /etc/bind/named.conf.local dies. Die IP-Adresse des Ubuntu-Slaves als zweiter Nameserver für Redundanz wird als Transfer angegeben.

```
zone "u10.cyberlab.fhnw.ch" {
        type master;
        file "/etc/bind/db.u10.cyberlab.fhnw.ch";
        allow-transfer { 192.168.97.81; };
};

zone "97.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192.168.97";
        allow-transfer { 192.168.97.81; };
};
```

Auf der Ubuntu-Slave genügt die Datei /etc/bind/named.conf.local, die Konfigurationsdaten der Zonen holt sich dieser vom ersten Nameserver.

```
zone "u10.cyberlab.fhnw.ch" {
        type slave;
        file "/var/cache/bind/db.u10.cyberlab.fhnw.ch";
        masters { 192.168.97.80; };
};

zone "97.168.192.in-addr.arpa" {
        type slave;
        file "/var/cache/bind/db.192.168.97";
        masters { 192.168.97.80; };
};
```

Es ist wichtig, sicherzustellen, dass die IP-Adressen der virtuellen Maschinen korrekt konfiguriert sind. Dies kann mithilfe von netplan und der Datei /etc/netplan/00-installer-config.yaml erfolgen. Hier ein Beispiel von der Ubuntu-DNS Machine:

```
network:
  ethernets:
    enp0s3:
      dhcp4: false
      addresses:
        - 192.168.97.80/22
      routes:
        - to: default
          via: 192.168.96.1
      nameservers:
        addresses: [192.168.97.80]
  version: 2
```

Nachdem die IP-Adresse korrekt eingestellt wurde, kann der Bind9-Dienst neu gestartet werden. Die Subdomäne u10.cyberlab.fhnw.ch ist jetzt einsatzbereit.

3 Mail-Server

Der Mail-Server wird auf einer weiteren virtuellen Maschine Ubunut-Mail aufgesetzt. Dazu wird der Dienst Postfix installiert.

Die Datei /etc/postfix/main.cf wird zur Konfiguration des Mail-Servers verwendet. Der Parameter myhostname setzt den Hostnamen, unter dem der Server im Netzwerk bekannt ist. Der Parameter mydomain definiert die Domäne des Mailservers. Der Eintrag home_mailbox gibt an, dass E-Mails in das Verzeichnis Maildir im Home-Verzeichnis des jeweiligen Benutzers zugestellt werden sollen. Der Parameter virtual_alias_maps ist für die Zuordnung von E-Mail-Adressen zu lokalen Benutzern zuständig. In der Datei /etc/postfix/virtual ist die Zuordnung damjan@u10.cyberlab.fhnw.ch damjan eingetragen. Das bedeutet, dass E-Mails an die Adresse damjan@u10.cyberlab.fhnw.ch im Ordner /home/damjan/Maildir abgespeichert werden.

```
myhostname = mail.u10.cyberlab.fhnw.ch
mydomain = u10.cyberlab.fhnw.ch

# Other configuration

home_mailbox = Maildir/
virtual_alias_maps = hash:/etc/postfix/virtual
```

Als Mail-Client wurde S-nail installiert. Es muss sichergestellt werden, dass die Umgebungsvariable für alle Benutzer auf MAIL=~/Maildir gesetzt ist. Nachdem S-nail installiert ist, wird die Datei /etc/s-nail.rc mit den folgenden Zeilen ergänzt.

```
set emptystart
set folder=Maildir
set record=+sent
```

Postfix muss neu gestartet werden. Es ist nun möglich, eine Mail an den Reflector des Cyberlab zu senden, z. B. echo 'Mail von u10' | s-nail -s 'u10 Testmail' -r damjan@u10.cyberlab.fhnw.ch reflector@cyberlab.fhnw.ch.

4 SPF/DKIM

Ein SPF-Record in der Datei /etc/bind/db.u10.cyberlab.fhnw.ch bestimmt, welche Mailserver dazu befugt sind, E-Mails in Vertretung dieser Domain zu versenden. Die Angabe mx erlaubt den Mailservern, die in den MX-Einträgen der Domain festgelegt sind, E-Mails zu verschicken. Die Verwendung von -all deutet an, dass sämtliche anderen Server, die nicht in den MX-Einträgen der Domain aufgeführt sind, keine Berechtigung haben, E-Mails im Namen dieser Domain zu senden.

```
u10.cyberlab.fhnw.ch.        IN      TXT     "v=spf1 mx -all"
```

Postfix muss so configuriert werden dass der SMTP Server SPF records von einkommenden Mails überprüft. Der Dienst postfix-policyd-spf-python wird installiert. Die Datei /etc/postfix/master.cf wird mit dem Eintrag erweitert:

```
policyd-spf unix -      n       n       -       0       spawn
        user=policyd-spf argv=/usr/bin/policyd-spf
```

Schliesslich wird auch das /etc/postfix/main.cf angepasst:

```
policyd-spf_time_limit = 3600
smtpd_recipient_restrictions =
        permit_mynetworks,
        permit_sasl_authenticated,
        reject_unauth_destination,
        check_policy_service unix:private/policyd-spf
```

Mit DKIM kann sichergestellt werden, dass eine E-Mail tatsächlich von der angegebenen Domain stammt und nicht gefälscht wurde. Der Absenders signiert jede ausgehende Nachricht mit einem privaten Schlüssel. Der Empfänger ruft den öffentlichen Schlüssel aus den DNS-Einträgen des Absenders ab und überprüft die Signatur.

Um DKIM umzusetzen wurde der Dienst Opendkim auf der Ubuntu-Mail Maschine installiert. Die Datei /etc/opendkim.conf sieht wie folgt aus:

```
OversignHeaders         From
TrustAnchorFile         /usr/share/dns/root.key
AutoRestart             yes
AutoRestartRate         10/1h
UMask                           002
Syslog                  yes
SyslogSuccess           yes
LogWhy                  yes
Canonicalization        relaxed/simple
ExternalIgnoreList  refile:/etc/opendkim/TrustedHosts
InternalHosts       refile:/etc/opendkim/TrustedHosts
KeyTable            refile:/etc/opendkim/KeyTable
SigningTable        refile:/etc/opendkim/SigningTable
Mode                sv
PidFile                 /var/run/opendkim/opendkim.pid
SignatureAlgorithm  rsa-sha256
UserID                  opendkim:opendkim
Socket              inet:12301@localhost
```

Unter /etc/default/opendkim muss die Zeile SOCKET=inet:12301@localhost hinzugefügt werden.
Die Datei /etc/postfix/main.cf wird mit folgenden Einträgen ergänzt:

```
milter_protocol = 2
milter_default_action = accept
smtpd_milters = inet:localhost:12301
non_smtpd_milters = inet:localhost:12301
```

Unter /etc/opendkim/TrustedHosts wird die Zeile *.cyberlab.fhnw.ch hinzugefügt. In der Datei /etc/opendkim/KeyTable wird der Pfad zum privaten Schlüssel zum signieren angegeben.

```
mail._domainkey.u10.cyberlab.fhnw.ch
u10.cyberlab.fhnw.ch:mail:/etc/opendkim/keys/u10.cyberlab.fhnw.ch/mail.private
```

In der Datei /etc/opendkim/SigningTable wir die Zeile *@u10.cyberlab.fhnw.ch mail._domainkey.u10.cyberlab.fhnw.ch hinzugefügt. Alle Mails von der Domäne u10.cyberlab.fhnw.ch werden mit dem privaten Schlüssel signiert.

Die Schlüsselpaare werden erstellt und unter /etc/opendkim/keys/u10.cyberlab.fhnw.ch abgespeichert. Der private Schlüssel ist in der Datei mail.private. Der öffentliche Schlüssel ist in der Datei mail.txt, damit wird der DKIM-Record erstellt. Postfix und Opendkim muss neu gestartet werden.

```
mail._domainkey.u10.cyberlab.fhnw.ch.   IN  TXT "v=DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwL/"
"AOUT0DLI9Y8zFRCd5AN+oJggpIoHcCvPngDkMOJzAhsN9i5vXOESzXm9KDt4u1CRpcwEruDT6UZZ2L0f6f2
Q7r5yt/"
"T4Vo/Do67nNIpUwoyEjeOURcDrLPTUx/mKocP7GOscQ6AAhNZHAYlMqMO426t29h7SQt1aHMdZYjqmmuk
VvdAN0R93jDJvbEuSzwk8FcPq0fm9fryqVWj6YfuvpsXQcpm556iX55QRLxlQJjp6JEAeDrBWAbxwGkI+Rdz/"
"vS+MY95p992F5mROxi1CB9aRTIWKt62IvtnjCVrZIfrB+Yoa9+nH5MWg8LNUHdPIv6+M2ik7wVURfkgmgv
wIDAQAB"
```

5 Greylisting

Greylisting ist eine Technik zur Reduzierung von Spam. Dabei werden E-Mails von unbekannten Absendern zunächst temporär abgelehnt. Mailserver versuchen dann, die E-Mail nach einem kurzen Zeitraum erneut zu senden, woraufhin die E-Mail angenommen und der Absender auf eine Liste bekannter Absender gesetzt wird, sodass zukünftige E-Mails sofort verarbeitet werden. Die meisten Spam-Mailer hingegen senden E-Mails nach einem fehlgeschlagenen Versuch nicht erneut.

Auf der Ubuntu-Mail Machine wird der Dienst Postgrey für die Umsetzung installiert. Die /etc/postfix/main.cf Datei wird angepasst:

```
policyd-spf_time_limit = 3600
smtpd_recipient_restrictions =
        permit_mynetworks,
        permit_sasl_authenticated,
        reject_unauth_destination,
        check_policy_service unix:private/policyd-spf
        check_policy_service inet:127.0.0.1:10023
```

Bestimmte E-Mails sollen jedoch nicht von Begin an abgelehnt werden. Dazu wurde eine Whitelist definiert. In der Datei /etc/default/postgrey wir die Ziele hinzugefügt, damit Postgrey die Whitelist beachtet.

```
POSTGREY_OPTS="--inet=127.0.0.1:10023 --whitelist-clients=/etc/postgrey/whitelist_clients.local"
```

In die Datei /etc/postgrey/whitelist_clients.local wird die Zeile cyberlab.fhnw.ch hineingeschrieben. E-Mails von dieser Domäne werden nicht abgelehnt. Postfix und Postgrey müssen neu gestartet werden.

6 Bayes

Die E-Mails müssen nun noch auf ihren Inhalt überprüft werden, um sicherzustellen, dass kein Virus über E-Mail empfangen wird. Amavis ist ein Filterprogramm, das eingehende E-Mails auf Spam und Viren überprüft. Es fungiert als Schnittstelle, die E-Mails entgegennimmt und zur weiteren Analyse an spezialisierte Programme weiterleitet. Zur Spam-Erkennung verwendet Amavis SpamAssassin. Für die Virenerkennung ruft Amavis ClamAV auf, ein Antivirenprogramm, das E-Mails auf Malware scannt.

Amavis, SpamAssassin und ClamAV werden auf der Ubuntu-Mail Machine installiert. Zusätzlich werden diverse Komprimierungsprogramme wie bzip2 installiert, damit Amavis in der Lage ist, Anhänge zu dekomprimieren. Die Datei /etc/amavis/conf.d/15-content_filter_mode bestimmt wie Amavis den E-Mail Inhalt filtert.

```
use strict;

@bypass_virus_checks_maps = (
  \%bypass_virus_checks, \@bypass_virus_checks_acl, \$bypass_virus_checks_re);

@bypass_spam_checks_maps = (
  \%bypass_spam_checks, \@bypass_spam_checks_acl, \$bypass_spam_checks_re);

1;
```

In der Datei /etc/postfix/main.cf wird die Zeile hinzugefügt.

```
content_filter = smtp-amavis:[127.0.0.1]:10024
```

Die Datei /etc/postfix/master.cf wird angepasst.

```
pickup    unix  n       -       y       60      1       pickup
        -o content_filter=
        -o receive_override_options=no_header_body_checks
# Other configuration...
smtp-amavis     unix    -       -       -       -       2       smtp
      -o smtp_data_done_timeout=1200
      -o smtp_send_xforward_command=yes
      -o disable_dns_lookups=yes
      -o max_use=20
127.0.0.1:10025 inet    n       -       -       -       -       smtpd
      -o content_filter=
      -o local_recipient_maps=
      -o relay_recipient_maps=
      -o smtpd_restriction_classes=
      -o smtpd_delay_reject=no
      -o smtpd_client_restrictions=permit_mynetworks,reject
      -o smtpd_helo_restrictions=
      -o smtpd_sender_restrictions=
      -o smtpd_recipient_restrictions=permit_mynetworks,reject
      -o smtpd_data_restrictions=reject_unauth_pipelining
      -o smtpd_end_of_data_restrictions=
      -o mynetworks=127.0.0.0/8
      -o smtpd_error_sleep_time=0
      -o smtpd_soft_error_limit=1001
      -o smtpd_hard_error_limit=1000
      -o smtpd_client_connection_count_limit=0
      -o smtpd_client_connection_rate_limit=0
      -o receive_override_options=no_header_body_checks,no_unknown_recipient_checks
```

In der Datei etc/amavis/conf.d/05-domain_id wird die Subdomain angegeben.

```
@local_domains_acl = ( ".$mydomain", ".u10.cyberlab.fhnw.ch" );
```

In die Datei etc/amavis/conf.d/50-user wird die Zeile eingefügt.

```
@whitelist_sender_acl = @local_domains_acl;
```

In die Datei etc/amavis/conf.d/05-node_id wird der Hostname angegeben.

```
$myhostname = "mail.u10.cyberlab.fhnw.ch";
```

Postfix und Amavis muss neu gestartet werden. Es soll auch sichergestellt werden, dass der ClamAV-Daemon läuft.

7 Absicherung überprüfen

Logs von /var/log/mail.log mit normalem Email von Reflector

```
Jun  1 09:20:08 postfix postfix/pickup[3037]: A3E0060673: uid=1000
from=<damjan@u10.cyberlab.fhnw.ch>
Jun  1 09:20:08 postfix postfix/cleanup[3129]: A3E0060673: message-id=<20240601092008.NL2L-
%damjan@u10.cyberlab.fhnw.ch>
Jun  1 09:20:08 postfix opendkim[774]: A3E0060673: DKIM-Signature field added (s=mail,
d=u10.cyberlab.fhnw.ch)
Jun  1 09:20:08 postfix postfix/qmgr[1604]: A3E0060673: from=<damjan@u10.cyberlab.fhnw.ch>,
size=440, nrcpt=1 (queue active)
Jun  1 09:20:08 postfix postfix/smtp[3130]: A3E0060673: to=<reflector@cyberlab.fhnw.ch>,
relay=srvMSG01.cyberlab.fhnw.ch[192.168.64.33]:25, delay=0.24, delays=0.07/0.01/0.06/0.1,
dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as DABC36011A)
Jun  1 09:20:08 postfix postfix/qmgr[1604]: A3E0060673: removed
Jun  1 09:20:09 postfix postfix/smtpd[3131]: connect from srvMSG01.cyberlab.fhnw.ch[192.168.64.33]
Jun  1 09:20:09 postfix policyd-spf[3132]: prepend Received-SPF: None (mailfrom) identity=mailfrom;
client-ip=192.168.64.33; helo=srvmsg01.cyberlab.fhnw.ch; envelope-
from=reflector@srvmsg01.cyberlab.fhnw.ch; receiver=<UNKNOWN>
Jun  1 09:20:09 postfix postgrey[989]: action=pass, reason=client whitelist,
client_name=srvMSG01.cyberlab.fhnw.ch, client_address=192.168.64.33/32,
sender=reflector@srvmsg01.cyberlab.fhnw.ch, recipient=damjan@u10.cyberlab.fhnw.ch
Jun  1 09:20:09 postfix postfix/smtpd[3131]: 2C0AB60671:
client=srvMSG01.cyberlab.fhnw.ch[192.168.64.33]
Jun  1 09:20:09 postfix postfix/cleanup[3129]: 2C0AB60671: message-
id=<20240601092009.076C06012B@srvMSG01.cyberlab.fhnw.ch>
Jun  1 09:20:09 postfix opendkim[774]: 2C0AB60671: srvMSG01.cyberlab.fhnw.ch [192.168.64.33] not
internal
Jun  1 09:20:09 postfix opendkim[774]: 2C0AB60671: not authenticated
Jun  1 09:20:09 postfix opendkim[774]: 2C0AB60671: no signature data
Jun  1 09:20:09 postfix postfix/qmgr[1604]: 2C0AB60671:
from=<reflector@srvmsg01.cyberlab.fhnw.ch>, size=4712, nrcpt=1 (queue active)
Jun  1 09:20:09 postfix postfix/smtpd[3131]: disconnect from
srvMSG01.cyberlab.fhnw.ch[192.168.64.33] ehlo=1 mail=1 rcpt=1 data=1 quit=1 commands=5
Jun  1 09:20:10 postfix postfix/smtpd[3136]: connect from localhost[127.0.0.1]
Jun  1 09:20:10 postfix postfix/smtpd[3136]: 3D03660673: client=localhost[127.0.0.1]
Jun  1 09:20:10 postfix postfix/cleanup[3129]: 3D03660673: message-
id=<20240601092009.076C06012B@srvMSG01.cyberlab.fhnw.ch>
Jun  1 09:20:10 postfix opendkim[774]: 3D03660673: no signing table match for
'reflector@srvmsg01.cyberlab.fhnw.ch'
Jun  1 09:20:10 postfix opendkim[774]: 3D03660673: no signature data
Jun  1 09:20:10 postfix postfix/qmgr[1604]: 3D03660673:
from=<reflector@srvmsg01.cyberlab.fhnw.ch>, size=5205, nrcpt=1 (queue active)
Jun  1 09:20:10 postfix postfix/local[3137]: 3D03660673: to=<damjan@u10.cyberlab.fhnw.ch>,
relay=local, delay=0.02, delays=0.01/0/0/0.01, dsn=2.0.0, status=sent (delivered to maildir)
Jun  1 09:20:10 postfix postfix/qmgr[1604]: 3D03660673: removed
Jun  1 09:20:10 postfix amavis[1627]: (01627-01) Passed CLEAN {RelayedInbound},
[192.168.64.33]:48860 <reflector@srvmsg01.cyberlab.fhnw.ch> -> <damjan@u10.cyberlab.fhnw.ch>,
Queue-ID: 2C0AB60671, Message-ID: <20240601092009.076C06012B@srvmsg01.cyberlab.fhnw.ch>,
mail_id: bPbNCGywhlkw, Hits: -0.999, size: 4677, queued_as: 3D03660673, 1067 ms
Jun  1 09:20:10 postfix postfix/smtp[3133]: 2C0AB60671: to=<damjan@u10.cyberlab.fhnw.ch>,
relay=127.0.0.1[127.0.0.1]:10024, delay=1.1, delays=0.06/0.01/0.01/1.1, dsn=2.0.0, status=sent (250
2.0.0 from MTA(smtp:[127.0.0.1]:10025): 250 2.0.0 Ok: queued as 3D03660673)
Jun  1 09:20:10 postfix postfix/qmgr[1604]: 2C0AB60671: removed
```

Test Email, welches von Reflector zurückgesendet wurde

```
From damjan@u10.cyberlab.fhnw.ch  Sat Jun  1 11:31:36 2024
Return-Path: <damjan@u10.cyberlab.fhnw.ch>
X-Original-To: reflector@cyberlab.fhnw.ch
Delivered-To: reflector@cyberlab.fhnw.ch
Received: from localhost (localhost [127.0.0.1])
        by srvMSG01.cyberlab.fhnw.ch (Postfix) with ESMTP id 5791A60122
        for <reflector@cyberlab.fhnw.ch>; Sat,  1 Jun 2024 11:31:36 +0200 (CEST)
Authentication-Results: srvmsg01.cyberlab.fhnw.ch (amavisd-new);
        dkim=pass (2048-bit key) header.d=u10.cyberlab.fhnw.ch
Received: from srvMSG01.cyberlab.fhnw.ch ([IPv6:::1])
        by localhost (srvmsg01.cyberlab.fhnw.ch [IPv6:::1]) (amavisd-new, port 10024)
        with ESMTP id inQEUjBPMGLZ for <reflector@cyberlab.fhnw.ch>;
        Sat,  1 Jun 2024 11:31:36 +0200 (CEST)
Received-SPF: Pass (mailfrom) identity=mailfrom; client-ip=192.168.97.189;
helo=mail.u10.cyberlab.fhnw.ch; envelope-from=damjan@u10.cyberlab.fhnw.ch;
receiver=<UNKNOWN>
Received: from mail.u10.cyberlab.fhnw.ch (unknown [192.168.97.189])
        by srvMSG01.cyberlab.fhnw.ch (Postfix) with ESMTPS id 3FD1F6011A
        for <reflector@cyberlab.fhnw.ch>; Sat,  1 Jun 2024 11:31:36 +0200 (CEST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=u10.cyberlab.fhnw.ch;
        s=mail; t=1717234296;
        bh=fA+/05Z0LbMk1N/rf8vAu7311wt082842KX3V/hHP3k=;
        h=Date:From:To:Subject:From;
        b=ASbZIJO0/1MFgrdICwRUqg07X2HKF3hvE03ZBZqyYgLGSfC3P/1IjGnWeDoHL1sIr
         b+NanJ/fnJhpXmjTXWyi3Zx/Ol6t+O7NYDe9Yw+26yrXuFMFq8ZsZvy59VSWZrGyS4
         DKR2RGXRuRdI/wRVY0KThFGGK9ffTnkb0ruIghVG+2IQc7nwS2Q6VRKq4zRUTBAkA+
         WGzUF/3THlIbN0sd0zR1s6Ms3jyFUrVEQ8yO2gjqqHalgVmVl5uirgh/kdqBrNhiCd
         VbcWRZgFn4jvup0/S8hFRI2mAPOIZRn6U6w0x1stscYjNitYvsZ4YRsSr4ihnxMXKQ
         cV9dSb00gZriw==
Received: by mail.u10.cyberlab.fhnw.ch (Postfix, from userid 1000)
        id 2027460676; Sat,  1 Jun 2024 09:31:36 +0000 (UTC)
Date: Sat, 01 Jun 2024 09:31:36 +0000
From: damjan@u10.cyberlab.fhnw.ch
To: reflector@cyberlab.fhnw.ch
Subject: clean
Message-ID: <20240601093136.cd26s%damjan@u10.cyberlab.fhnw.ch>
User-Agent: s-nail v14.9.23

Dies ist eine Nachricht von Damjan Mlinar an den Reflector von Cyberlab
```

Logs von /var/log/mail.log mit Virus-Email von Reflector

```
Jun  1 09:18:25 postfix postfix/pickup[3037]: 9809760673: uid=1000
from=<damjan@u10.cyberlab.fhnw.ch>
Jun  1 09:18:25 postfix postfix/cleanup[3074]: 9809760673: message-
id=<20240601091825.kmRPh%damjan@u10.cyberlab.fhnw.ch>
Jun  1 09:18:25 postfix opendkim[774]: 9809760673: DKIM-Signature field added (s=mail,
d=u10.cyberlab.fhnw.ch)
Jun  1 09:18:25 postfix postfix/qmgr[1604]: 9809760673: from=<damjan@u10.cyberlab.fhnw.ch>,
size=440, nrcpt=1 (queue active)
Jun  1 09:18:25 postfix postfix/smtp[3076]: 9809760673: to=<reflector@cyberlab.fhnw.ch>,
relay=srvMSG01.cyberlab.fhnw.ch[192.168.64.33]:25, delay=0.12, delays=0.06/0/0.02/0.04,
dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as B284E6011A)
Jun  1 09:18:25 postfix postfix/qmgr[1604]: 9809760673: removed
Jun  1 09:18:27 postfix postfix/smtpd[3099]: connect from srvMSG01.cyberlab.fhnw.ch[192.168.64.33]
Jun  1 09:18:27 postfix policyd-spf[3103]: prepend Received-SPF: None (mailfrom) identity=mailfrom;
client-ip=192.168.64.33; helo=srvmsg01.cyberlab.fhnw.ch; envelope-
from=reflector@srvmsg01.cyberlab.fhnw.ch; receiver=<UNKNOWN>
Jun  1 09:18:27 postfix postgrey[989]: action=pass, reason=client whitelist,
client_name=srvMSG01.cyberlab.fhnw.ch, client_address=192.168.64.33/32,
sender=reflector@srvmsg01.cyberlab.fhnw.ch, recipient=damjan@u10.cyberlab.fhnw.ch
Jun  1 09:18:27 postfix postgrey[989]: cleaning up old logs...
Jun  1 09:18:27 postfix postfix/smtpd[3099]: 413BE60672:
client=srvMSG01.cyberlab.fhnw.ch[192.168.64.33]
Jun  1 09:18:27 postfix postfix/cleanup[3074]: 413BE60672: message-
id=<20240601091826.D04496012B@srvMSG01.cyberlab.fhnw.ch>
Jun  1 09:18:27 postfix opendkim[774]: 413BE60672: srvMSG01.cyberlab.fhnw.ch [192.168.64.33] not
internal
Jun  1 09:18:27 postfix opendkim[774]: 413BE60672: not authenticated
Jun  1 09:18:27 postfix opendkim[774]: 413BE60672: no signature data
Jun  1 09:18:27 postfix postfix/qmgr[1604]: 413BE60672:
from=<reflector@srvmsg01.cyberlab.fhnw.ch>, size=5133, nrcpt=1 (queue active)
Jun  1 09:18:27 postfix postfix/smtpd[3099]: disconnect from
srvMSG01.cyberlab.fhnw.ch[192.168.64.33] ehlo=1 mail=1 rcpt=1 data=1 quit=1 commands=5
Jun  1 09:18:28 postfix amavis[1626]: (01626-01) Blocked INFECTED (Win.Test.EICAR_HDB-1)
{DiscardedInbound,Quarantined}, [192.168.64.33]:57864 <reflector@srvmsg01.cyberlab.fhnw.ch> ->
<damjan@u10.cyberlab.fhnw.ch>, quarantine: 7/virus-7AueO3MCQ0Xg, Queue-ID: 413BE60672,
Message-ID: <20240601091826.D04496012B@srvmsg01.cyberlab.fhnw.ch>, mail_id:
7AueO3MCQ0Xg, Hits: -, size: 5098, 981 ms
Jun  1 09:18:28 postfix postfix/smtp[3104]: 413BE60672: to=<damjan@u10.cyberlab.fhnw.ch>,
relay=127.0.0.1[127.0.0.1]:10024, delay=1.2, delays=0.19/0.01/0.23/0.82, dsn=2.7.0, status=sent
(250 2.7.0 Ok, discarded, id=01626-01 - INFECTED: Win.Test.EICAR_HDB-1)
Jun  1 09:18:28 postfix postfix/qmgr[1604]: 413BE60672: removed
```

8 Anhang

db.u10.cyberlab.fhnw.ch

```
$TTL 10800 ; 3 Stunden in Sekunden
u10.cyberlab.fhnw.ch. IN SOA ns1.u10.cyberlab.fhnw.ch. hostmaster.u10.cyberlab.fhnw.ch. (
                                1         ; Serial
                                10800 ; Refresh after 3 hours
                                3600   ; Retry after 1 hour
                                604800         ; Expire after 1 week
                                3600   ; Negativ caching TTL of 1
)

; Nameserver
u10.cyberlab.fhnw.ch.        IN      NS      ns1.u10.cyberlab.fhnw.ch.
u10.cyberlab.fhnw.ch.        IN      NS      ns2.u10.cyberlab.fhnw.ch.

; Mailserver
u10.cyberlab.fhnw.ch.        IN      MX      10 mail.u10.cyberlab.fhnw.ch.

; Hosts
ns1.u10.cyberlab.fhnw.ch.   IN      A       192.168.97.80
ns2.u10.cyberlab.fhnw.ch.   IN      A       192.168.97.81
mail.u10.cyberlab.fhnw.ch.  IN      A       192.168.97.189

; SPF Record
u10.cyberlab.fhnw.ch.        IN      TXT     "v=spf1 mx -all"

; DKIM Record
mail._domainkey.u10.cyberlab.fhnw.ch.   IN  TXT "v=DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwL/"
"AOUT0DLI9Y8zFRCd5AN+oJggpIoHcCvPngDkMOJzAhsN9i5vXOESzXm9KDt4u1CRpcwEruDT6UZZ2
L0f6f2Q7r5yt/"
"T4Vo/Do67nNlpUwoyEjeOURcDrLPTUx/mKocP7GOscQ6AAhNZHAYlMqMO426t29h7SQt1aHMdZYjq
mmukVvdAN0R93jDJvbEuSzwk8FcPq0fm9fryqVWj6YfuvpsXQcpm556iX55QRLxlQJjp6JEAeDrBWAbxw
GkI+Rdz/"
"vS+MY95p992F5mROxi1CB9aRTIWKt62lvtnjCVrZIfrB+Yoa9+nH5MWg8LNUHdPIv6+M2ik7wVURfk
gmgvwIDAQAB"
```

main.cf

```
# myorigin = /etc/mailname

smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
biff = no

# appending .domain is the MUA's job.
append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

readme_directory = no

# See http://www.postfix.org/COMPATIBILITY_README.html -- default to 3.6 on
# fresh installs.
compatibility_level = 3.6

# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_tls_security_level=may

smtp_tls_CApath=/etc/ssl/certs
smtp_tls_security_level=may
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = mail.u10.cyberlab.fhnw.ch
mydomain = u10.cyberlab.fhnw.ch

alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, $mydomain, postfix, localhost.localdomain, localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
home_mailbox = Maildir/
virtual_alias_maps = hash:/etc/postfix/virtual

# SPF / Greylisting
policyd-spf_time_limit = 3600
smtpd_recipient_restrictions =
        permit_mynetworks,
        permit_sasl_authenticated,
        reject_unauth_destination,
        check_policy_service unix:private/policyd-spf
        check_policy_service inet:127.0.0.1:10023

#DKIM
milter_protocol = 2
milter_default_action = accept
smtpd_milters = inet:localhost:12301
non_smtpd_milters = inet:localhost:12301

#AMAVIS
content_filter = smtp-amavis:[127.0.0.1]:10024
```

master.cf

```
# Postfix master process configuration file.  For details on the format
# of the file, see the master(5) manual page (command: "man 5 master" or
# on-line: http://www.postfix.org/master.5.html).
#
# Do not forget to execute "postfix reload" after editing this file.
#
#
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (no)    (never) (100)
#
# ==========================================================================
smtp      inet  n       -       y       -       -       smtpd
#smtp      inet  n       -       y       -       1       postscreen
#smtpd     pass  -       -       y       -       -       smtpd
#dnsblog   unix  -       -       y       -       0       dnsblog
#tlsproxy  unix  -       -       y       -       0       tlsproxy
# Choose one: enable submission for loopback clients only, or for any client.
#127.0.0.1:submission inet n -   y       -       -       smtpd
#submission inet n       -       y       -       -       smtpd
#  -o syslog_name=postfix/submission
#  -o smtpd_tls_security_level=encrypt
#  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_tls_auth_only=yes
#  -o smtpd_reject_unlisted_recipient=no
#  -o smtpd_client_restrictions=$mua_client_restrictions
#  -o smtpd_helo_restrictions=$mua_helo_restrictions
#  -o smtpd_sender_restrictions=$mua_sender_restrictions
#  -o smtpd_recipient_restrictions=
#  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
# Choose one: enable smtps for loopback clients only, or for any client.
#127.0.0.1:smtps inet n  -       y       -       -       smtpd
#smtps     inet  n       -       y       -       -       smtpd
#  -o syslog_name=postfix/smtps
#  -o smtpd_tls_wrappermode=yes
#  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_reject_unlisted_recipient=no
#  -o smtpd_client_restrictions=$mua_client_restrictions
#  -o smtpd_helo_restrictions=$mua_helo_restrictions
#  -o smtpd_sender_restrictions=$mua_sender_restrictions
#  -o smtpd_recipient_restrictions=
#  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
#628       inet  n       -       y       -       -       qmqpd
pickup    unix  n       -       y       60      1       pickup
          -o content_filter=
          -o receive_override_options=no_header_body_checks
cleanup   unix  n       -       y       -       0       cleanup
qmgr      unix  n       -       n       300     1       qmgr
#qmgr     unix  n       -       n       300     1       oqmgr
tlsmgr    unix  -       -       y       1000?   1       tlsmgr
rewrite   unix  -       -       y       -       -       trivial-rewrite
bounce    unix  -       -       y       -       0       bounce
defer     unix  -       -       y       -       0       bounce
trace     unix  -       -       y       -       0       bounce
verify    unix  -       -       y       -       1       verify
flush     unix  n       -       y       1000?   0       flush
proxymap  unix  -       -       n       -       -       proxymap
proxywrite unix -       -       n       -       1       proxymap
```

```
smtp      unix  -       -       y       -       -       smtp
relay     unix  -       -       y       -       -       smtp
        -o syslog_name=postfix/$service_name
#       -o smtp_helo_timeout=5 -o smtp_connect_timeout=5
showq     unix  n       -       y       -       -       showq
error     unix  -       -       y       -       -       error
retry     unix  -       -       y       -       -       error
discard   unix  -       -       y       -       -       discard
local     unix  -       n       n       -       -       local
virtual   unix  -       n       n       -       -       virtual
lmtp      unix  -       -       y       -       -       lmtp
anvil     unix  -       -       y       -       1       anvil
scache    unix  -       -       y       -       1       scache
postlog   unix-dgram n  -       n       -       1       postlogd
#
#
==========================================================================
# Interfaces to non-Postfix software. Be sure to examine the manual
# pages of the non-Postfix software to find out what options it wants.
#
# Many of the following services use the Postfix pipe(8) delivery
# agent.  See the pipe(8) man page for information about ${recipient}
# and other message envelope options.
#
==========================================================================
#
# maildrop. See the Postfix MAILDROP_README file for details.
# Also specify in main.cf: maildrop_destination_recipient_limit=1
#
maildrop  unix  -       n       n       -       -       pipe
  flags=DRXhu user=vmail argv=/usr/bin/maildrop -d ${recipient}
#
#
==========================================================================
#
# Recent Cyrus versions can use the existing "lmtp" master.cf entry.
#
# Specify in cyrus.conf:
#   lmtp    cmd="lmtpd -a" listen="localhost:lmtp" proto=tcp4
#
# Specify in main.cf one or more of the following:
#  mailbox_transport = lmtp:inet:localhost
#  virtual_transport = lmtp:inet:localhost
#
#
==========================================================================
#
# Cyrus 2.1.5 (Amos Gouaux)
# Also specify in main.cf: cyrus_destination_recipient_limit=1
#
#cyrus     unix  -       n       n       -       -       pipe
#  flags=DRX user=cyrus argv=/cyrus/bin/deliver -e -r ${sender} -m ${extension} ${user}
#
#
==========================================================================
# Old example of delivery via Cyrus.
#
#old-cyrus unix  -       n       n       -       -       pipe
#  flags=R user=cyrus argv=/cyrus/bin/deliver -e -m ${extension} ${user}
#
#
```

```
==========================================================================
======
#
# See the Postfix UUCP_README file for configuration details.
#
uucp      unix  -       n       n       -       -       pipe
  flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail ($recipient)
#
# Other external delivery methods.
#
ifmail    unix  -       n       n       -       -       pipe
  flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nexthop ($recipient)
bsmtp     unix  -       n       n       -       -       pipe
  flags=Fq. user=bsmtp argv=/usr/lib/bsmtp/bsmtp -t$nexthop -f$sender $recipient
scalemail-backend unix -       n       n       -       2       pipe
  flags=R user=scalemail argv=/usr/lib/scalemail/bin/scalemail-store ${nexthop} ${user} $
{extension}
mailman   unix  -       n       n       -       -       pipe
  flags=FRX user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py ${nexthop} ${user}

policyd-spf unix -      n       n       -       0       spawn
          user=policyd-spf argv=/usr/bin/policyd-spf
smtp-amavis     unix    -       -       -       -       2       smtp
        -o smtp_data_done_timeout=1200
        -o smtp_send_xforward_command=yes
        -o disable_dns_lookups=yes
        -o max_use=20

127.0.0.1:10025 inet    n       -       -       -       -       smtpd
        -o content_filter=
        -o local_recipient_maps=
        -o relay_recipient_maps=
        -o smtpd_restriction_classes=
        -o smtpd_delay_reject=no
        -o smtpd_client_restrictions=permit_mynetworks,reject
        -o smtpd_helo_restrictions=
        -o smtpd_sender_restrictions=
        -o smtpd_recipient_restrictions=permit_mynetworks,reject
        -o smtpd_data_restrictions=reject_unauth_pipelining
        -o smtpd_end_of_data_restrictions=
        -o mynetworks=127.0.0.0/8
        -o smtpd_error_sleep_time=0
        -o smtpd_soft_error_limit=1001
        -o smtpd_hard_error_limit=1000
        -o smtpd_client_connection_count_limit=0
        -o smtpd_client_connection_rate_limit=0
        -o receive_override_options=no_header_body_checks,no_unknown_recipient_checks
```