Wie richte ich einen sicheren Mailserver ein?

Intention

Dieses Pattern erläutert die verfügbaren Möglichkeiten um den eigenen Mailserver abzusichern.

Problemstellung

Sichere Kommunikation und Datenintegrität ist für viele Personen wichtig. Gerade im Mailverkehr will man sicher gehen, dass man keinen schlechten Eindruck hinterlässt oder dass die eigenen Mails nicht im Spam-Ordner des Empfängers landen. Ob die Mails im Spam-Ordner des Empfängers landen, hängt oft mit der Sicherheit des Mailservers zusammen.

Szenario

Eine Mailadresse, die der eigenen Webadresse zugeordnet werden kann, soll eingerichtet werden. Wie setzt man nun so einen Maildienst sicher auf dem eigenen Server auf?

Lösung

Bevor man einen eigenen Mailserver einrichtet, sollte man das Pattern „Sollte ich einen Mailserver selbst einrichten oder betreiben?“ durchlesen. Denn das Einrichten und Betreiben eines Mailservers ist aufwendig und komplex.

Begriffsdefinitionen

SMTP ist die Kurzform für Simple Mail Transfer Protocol und versendet die Mails vom Server. **IMAP** und **POP3** sind die Übertragungsprotokolle, die benutzt werden um die Mails mit einem Mailprogramm vom Server abzuholen.
Falls eine Mailsoftware auf dem Server installiert ist, kann Punkt 1 **übersprungen werden.**

1. Mail-Applikation auf dem Server installieren

Unabhängig davon, welche Mail-Applikation verwendet werden soll, sollten folgende Angelegenheiten vorher abgeklärt werden:

- Die Voraussetzungen für den Einsatz der Software müssen gegeben sein
    - Es kann immer nur eine SMTP-Applikation pro Server verwenden werden
- Auf Inkompatibilitäten achten
    - Wenn vorher eine andere SMTP-Applikation installiert war, muss diese vollständig entfernt werden
- Aktualität und Updatefrequenz der zu verwendenden SMTP-Applikation beachten
    - Man möchte auch in den kommenden Jahren auf dem aktuellsten Stand sein und sich darauf verlassen können, dass Sicherheitslecks schnell gepatcht werden.

Es empfiehlt sich, das IMAP-Protokoll zu benutzen, da hierbei eine Synchronisation zwischen Client (Mailprogramm auf dem Smartphone oder PC) und dem Server stattfindet. Somit hat man immer den aktuellsten Stand und Zugriff auf allen Geräten.

2. Mailserver absichern

Folgendes ist IMMER zu beachten!

- NIEMALS die Standardeinstellungen (default settings) verwenden
- Die Standardpasswörter sofort ändern
- Passwörter (vor allem für Admin-Accounts) in regelmäßigen Abständen ändern
    - Mehr zum Thema Passwörter findet man im Pattern „**Wie sieht ein guter und sicherer Webshop aus?**“ in den Sektionen „Lösung“ und „Beispiele“.
- Alle Einstellungen, Konfigurationen und Funktionen sollten vorher getestet werden
- Regelmäßig die Funktionalität und Sicherheit des Mailservers testen

Nachdem nun eine beliebige Mail-Applikation auf dem Server installiert wurde oder schon vorhanden ist, sollten folgende Einstellungen in der Konfiguration vorgenommen werden um den Mailserver abzusichern:

- SSL / TLS Verschlüsselung aktivieren
- SSLv2 und SSLv3 deaktivieren
- SMTP-AUTH aktivieren
- TSL Verschlüsselung für ein- und ausgehende Mails aktivieren
- Anzahl der möglichen Verbindungen reduzieren um DDoS Attacken abzumildern
- Die Anzahl für fehlgeschlagenen Login-Versuche heruntersetzen
- DNS Blacklists nutzen um Spam-Mails abzufangen
- Reverse DNS LookUp nutzen um den Absender zu verifizieren
- SPF (Sender Policy Framework) aktivieren
- Lokale Blacklist erstellen, die spezifisch die IP-Adressen blockieren die nicht in den DNS Blacklists stehen

Beispiele

Eine gute Anleitung zum Einrichten des Mailservers

- https://workaround.org/ispmail

rspam – Ani Spam Tool

- https://www.openhub.net/p/10349

Postfix auf RedHat installieren (englisch)

- https://tecadmin.net/install-and-configure-postfix-on-centos-redhat/

Postfix auf Ubuntu installieren (englisch)

- https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-postfix-on-ubuntu-16-04

Postfix mit Let's Encrypt (SSL) absichern

- https://www.upcloud.com/support/secure-postfix-using-lets-encrypt/

Weitere Anleitungen zur Installation von Mailservern mit Absicherung (englisch)

- https://www.codeproject.com/Articles/847650/How-to-Install-Configure-Email-Server-with-Postfix

SMTP-Authentifikation für Postfix (englisch)

- http://postfix.state-of-mind.de/patrick.koetter/smtpauth/smtp_auth_mailclients.html

DNS Blacklist in Postfix

- https://docs.iredmail.org/enable.dnsbl.html

Weitere Absicherung für Postfix (Anzahl maximaler Verbindungen, usw.)

- http://www.postfix.org/TUNING_README.html

SSL / TLS Verschlüsselung

- Im Pattern „**Wie verschlüssele ich die Kommunikation mit meiner Website?**" ist erklärt, wie man ein SSL-Zertifikat erhält. Sofern keine Subdomain (mail.ihreseite.at) verwendet

wird, sondern der Mailserver mit derselben Domain (ihreseite.at) läuft, kann dasselbe Zertifikat verwendet werden.
- Hierzu muss nur der DNS MX Eintrag (record) der Mail-Applikation von @mail.ihreseite.at auf @ihreseite.at geändert werden.

SMTP Diagnose Tool **um die eigene SMTP-Konfiguration zu testen**

- https://mxtoolbox.com/diagnostic.aspx

Spam mit DNS Blacklists blockieren

Konfiguration für postfix (http://www.postfix.org)

```
smtpd_sender_restrictions =

  permit_mynetworks,

  permit_sasl_authenticated,

  reject_unknown_sender_domain,

  reject_non_fqdn_sender

smtpd_recipient_restrictions =

  permit_mynetworks,

  permit_sasl_authenticated,

  reject_unauth_destination,

  reject_unauth_pipelining,

  check_client_access hash:/etc/postfix/client_checks,

  check_sender_access hash:/etc/postfix/sender_checks,

  reject_unknown_helo_hostname,

  reject_invalid_hostname,

  reject_non_fqdn_hostname,

  reject_non_fqdn_recipient,

  permit_dnswl_client list.dnswl.org,
```

```
    reject_rbl_client ix.dnsbl.manitu.net,

    reject_rbl_client zen.spamhaus.org,

    reject_rbl_client b.barracudacentral.org,

    reject_rbl_client bl.spamcop.net,

    reject_rbl_client psbl.surriel.com,

    reject_rbl_client noptr.spamrats.com,

    reject_rbl_client dyna.spamrats.com,

    reject_rbl_client dnsbl.sorbs.net
```

Referenzen

https://www.upcloud.com/support/secure-postfix-using-lets-encrypt/
https://webmasters.stackexchange.com/questions/83442/single-ssl-certificate-for-web-and-email
https://wiki.archlinux.org/index.php/Virtual_user_mail_system
https://workaround.org/ispmail/jessie
https://www.howtoforge.com/effective_mail_server_defense
https://www.syn-flut.de/mit-postfix-spam-blockieren
https://blog.returnpath.com/blacklist-basics-the-top-email-blacklists-you-need-to-know-v2/
https://www.alienvault.com/blogs/security-essentials/basic-best-practices-for-configuring-email-servers
https://www.linode.com/docs/email/postfix/postfix-smtp-debian7/
http://www.postfix.org/BASIC_CONFIGURATION_README.html

Keywords

E-Mail, Mailserver, Security, SMTP, POP3, IMAP