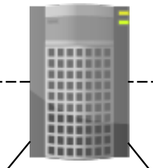
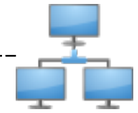
Internet



VM RZ

Firewall



Container

Container

Mail-Server

Generell kein Spamschutz
Keine Überprüfung der Authentiztät
Anonymes Versenden von Mails erlauben
Persistieren der Mails für zukünftige Analyse

Ausgehende Mails analysieren

Herausfinden woher die Mail kommt (über IP - Adresse des Nutzers des Relays)
Wie häufig / in welchem Interval hat dieser Nutzer / IP eine Spam-Mail versendet
An wie viele Adressen sind Spam-Mails im Schnitt gerichtet
An welche Zielgruppen ist Spam grob gerichtet
Kann man per Fingerprinting häufig genutzte OS herausfinden
Gibt es einen abrubten Stop des Services durch eine Anti-Spam-Service-Liste

Eingehende Mails analysieren

Herausfinden woher Mails kommen
Automatisches Anklicken der Links in den Spam Mails um mehr Spam zu bekommen
Generisch auf Spam antworten, um mehr Spam zu bekommen / zu sehen ob Mensch oder Maschine
Ist der Sender der Mail bereits auf einer Blacklist
Registrieren mit verschiedenen Präfixen auf zweifelhaften Services um zu sehen wer weiter gibt
Sind lustige Spam-Mails vorhanden?
Was sind die aktuellen Methoden von Spam / Phishing?

DNS-Server

Bereitstellung einer Domain
Validation des Mail-Servers