DFN
Deutsches Forschungsnetz

Abwehr von Spam und Malware in E-Mails

Christian Grimm

DFN-Nutzergruppe Hochschulverwaltung
10. Mai 2010, Berlin

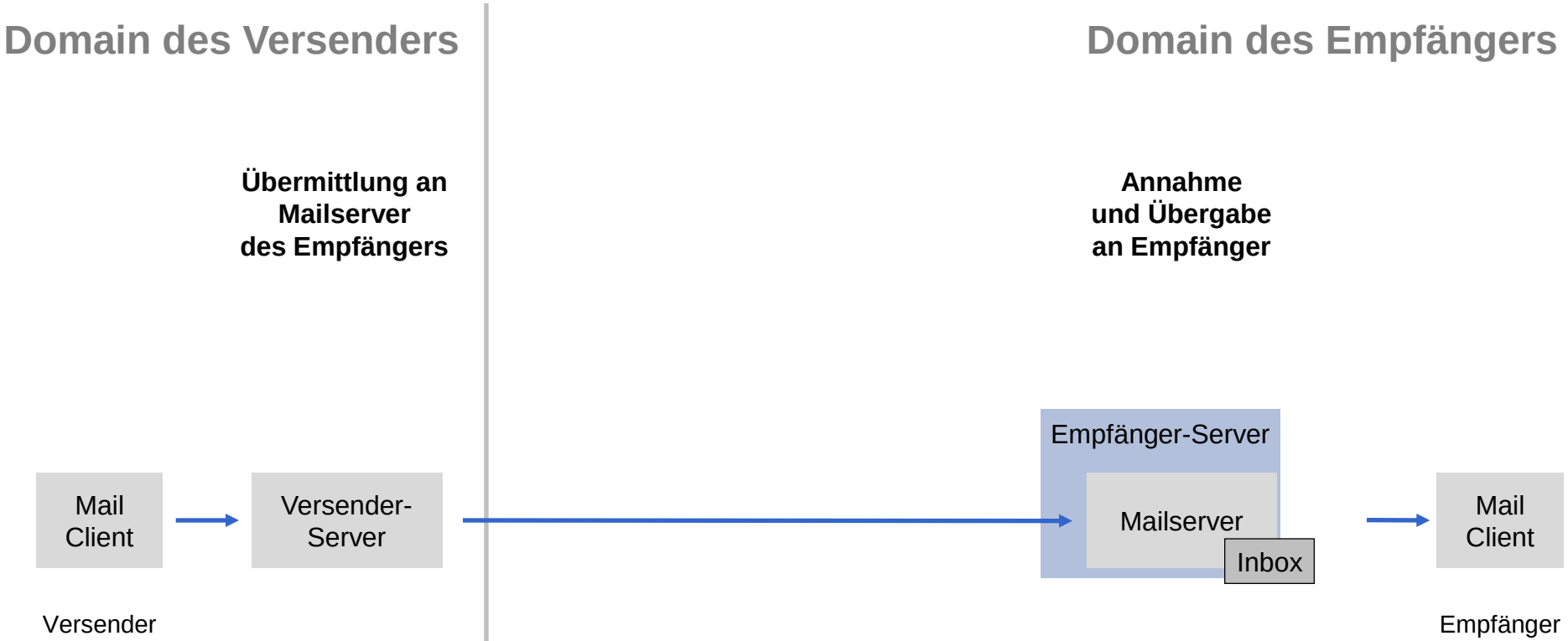
Übersicht

- Bedeutung von E-Mail
- Risiken im Umgang mit E-Mail
- Maßnahmen zum Schutz vor verseuchten E-Mails
- DFN-Dienst zur Abwehr verseuchter E-Mails

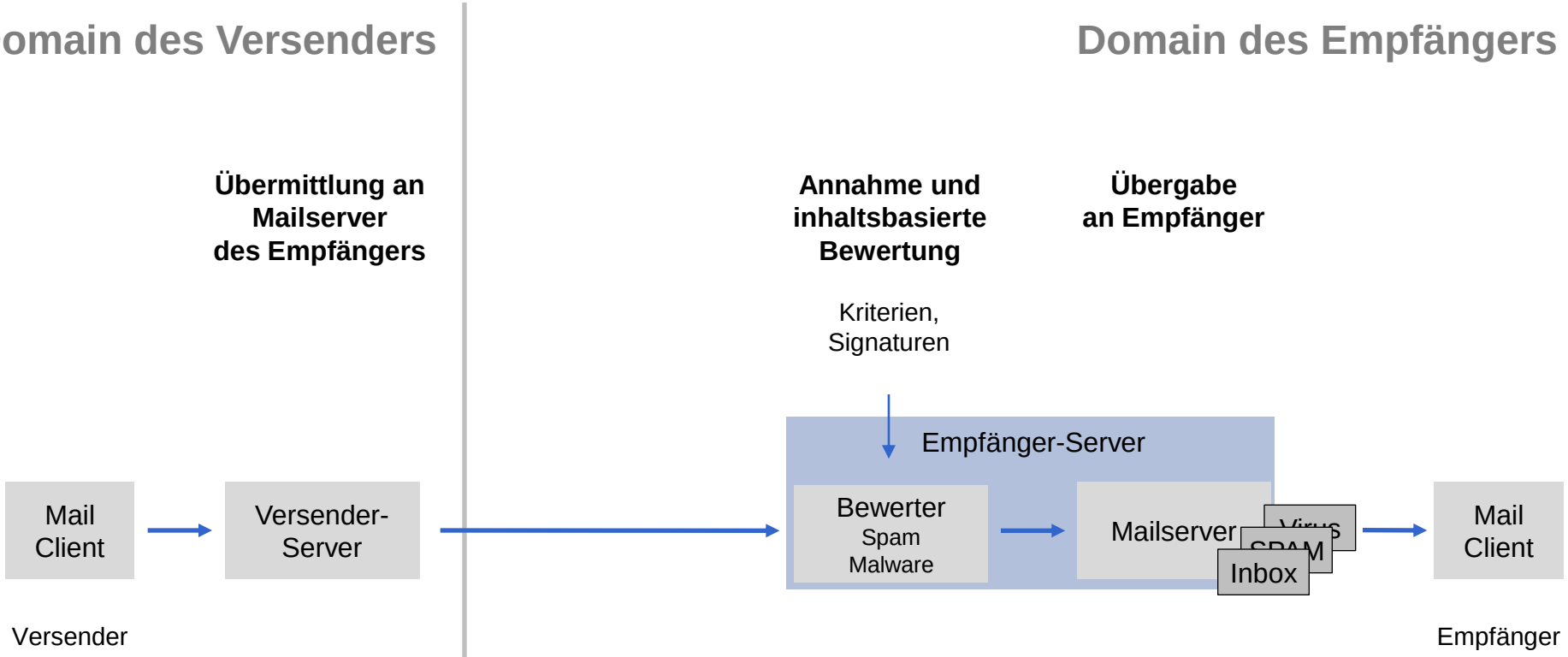
Bedeutung von E-Mail

- In Geschäftsprozessen mittlerweile fest etabliertes Werkzeug der Kommunikation
- Angreifer erhalten über E-Mail direkten Kontakt zu den Nutzern
- Anzahl „unbedarfter Angriffe“ sinkt –
  aber Nutzung von E-Mail und zielgerichtete Angriffe nehmen weiter zu
- E-Mail wird auch langfristig kritisches Einfallstor für Angreifer bleiben

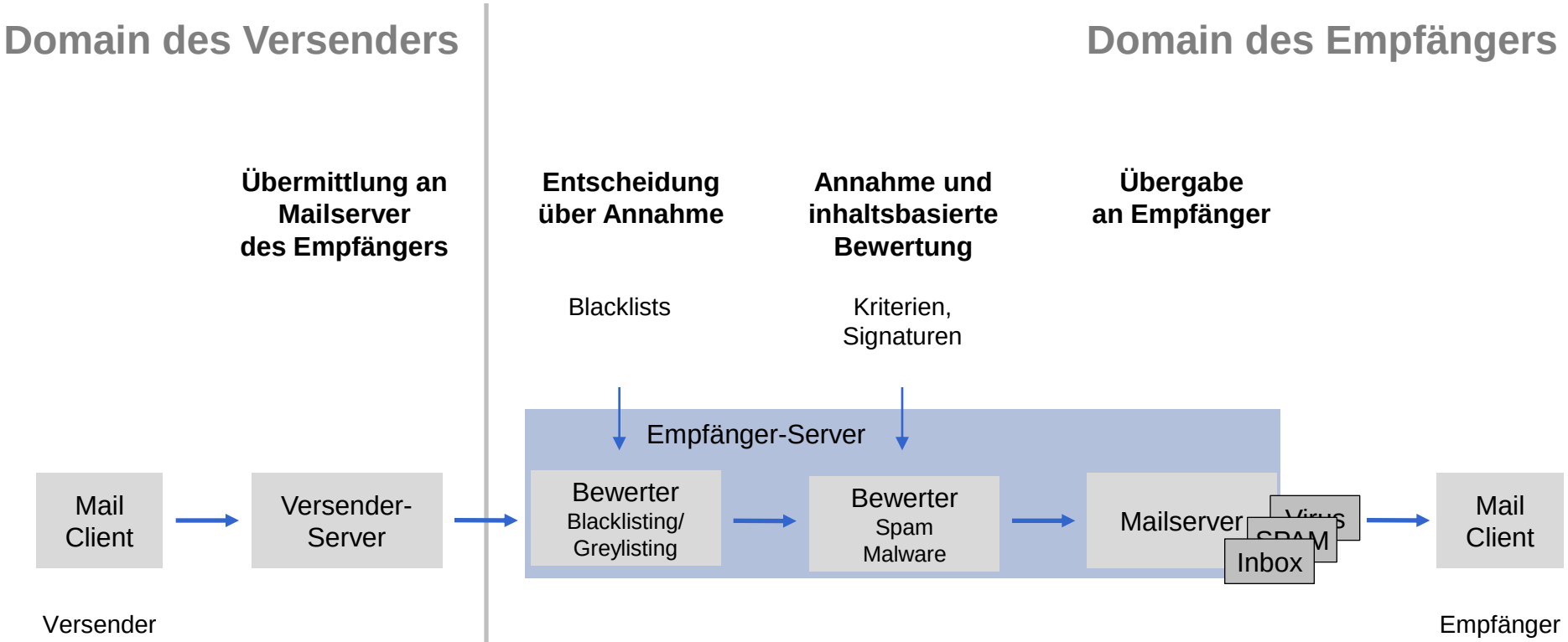
E-Mail-Transfer ohne Filter



E-Mail-Transfer mit Filter (1)



E-Mail-Transfer mit Filter (2)



Zahlenbeispiel

- Statistik für einen Tag im DFN
  - E-Mails an Mitarbeiter DFN und im Dienst WinShuttle

- 2.144.864 Zustellversuche „von außen“
  - 2.098.508 (97,84%) abgewiesen
    - 1.665.496 (77,65%) durch Blacklisting
    - 433.012 (20,19%) wegen „User unknown“
  - 46.356 (2,16%) angenommen und verarbeitet
    - 14.414 (0,67%) Inhalt positiv auf Spam oder Malware erkannt
    - 31.942 (1,49%) unbeanstandet!

sinkt

steigt

steigt

steigt

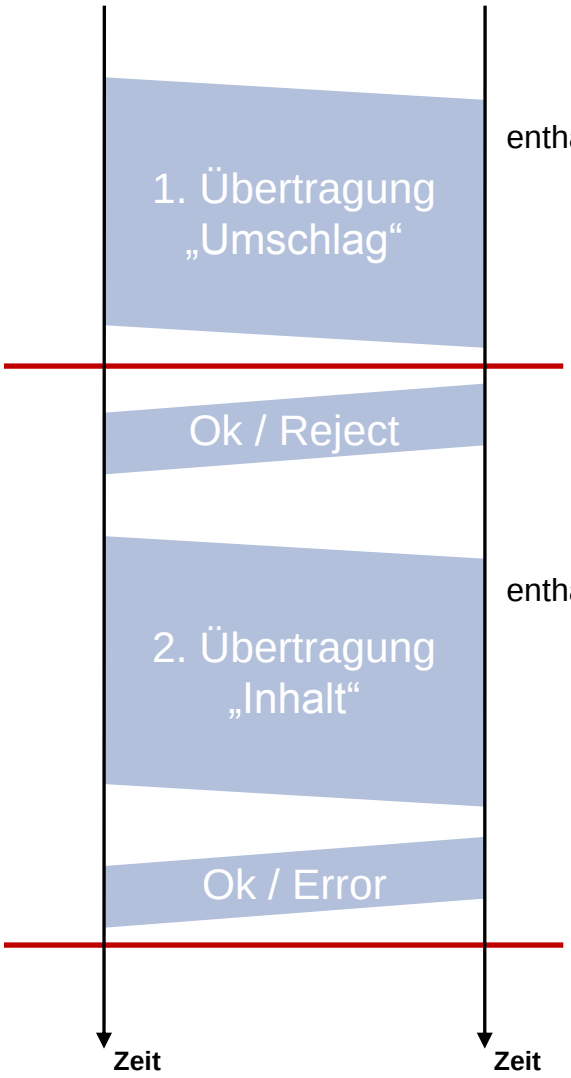
- Tendenzen

Zwischenstand

- Abwehr verseuchter E-Mails erfolgt zweistufig
  1. Entscheidung über Annahme von Mails
     - Blacklisting und/oder Greylisting
     - basiert auf IP- und E-Mail-Adressen
  2. Bewertung angenommener E-Mails auf Spam/Malware
     - Untersuchung des Inhalts von E-Mails
     - Markierung des Ergebnisses im Header der E-Mails

- Auch rechtlich sind beide Schritte getrennt zu bewerten!
  – maßgeblich ist Zeitpunkt der Annahme einer E-Mail

Zeitl. Ablauf Übertragung E-Mail



enthält:
Adresse des Versender-Servers
E-Mail-Adresse des Versenders
E-Mail-Adresse des Empfängers

hier: Entscheidung über Annahme durch Blacklisting oder Greylisting

enthält:
Header und Body der Mail, unter anderem
Betreff:
Datum:
Inhalt
Attachments

hier: Inhaltsbasierte Bewertung nach Annahme

Kriterien Juristische Bewertung Blacklisting / Greylisting

DFN Deutsches Forschungsnetz

- TKG+TMG: Datenschutz
  - Erheben und Umgang mit personenbezogenen Daten
- TKG: Fernmeldegeheimnis
  - § 88: Inhalt und nähere Umstände der Kommunikation
- StGB: Fernmeldegeheimnis und Datenveränderung
  - § 206: Verletzung Fernmeldegeheimnis – hier Anvertrauen
  - § 303a: Datenveränderung – hier Unterdrückung
- Zivilrecht: Pflichten aus Nutzungsverhältnis
  - Pflicht zur Weitergabe aller E-Mails?
- PersVG: Mitbestimmung des Personalrats
  - Überwachung möglich?
- Informationspflichten ggü. Versender und Empfänger

Ergebnis Juristische Bewertung Blacklisting / Greylisting

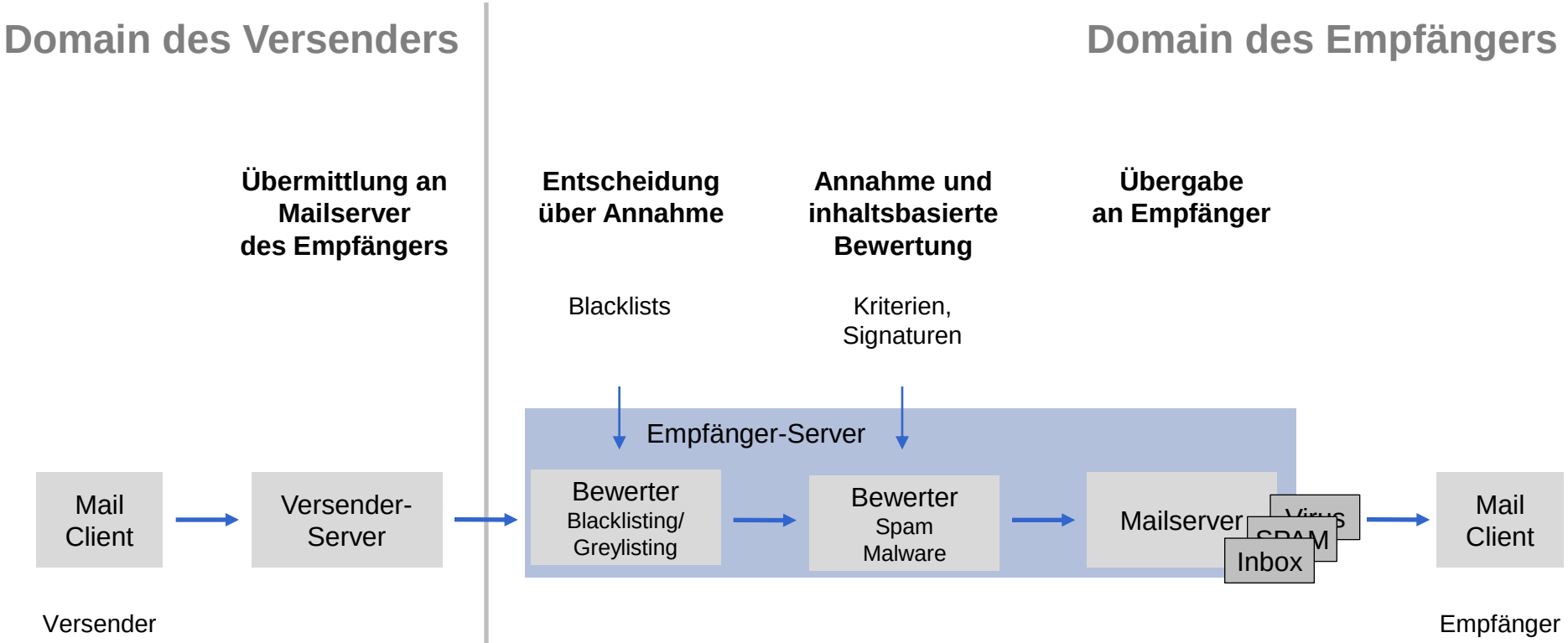
DFN Deutsches Forschungsnetz

	Blacklisting	Greylisting
Datenschutz	Nicht einschlägig	nach § 100 I TKG gerechtfertigt
Fernmeldegeheimnis	Nicht einschlägig	nach § 88 III 1 TKG gerechtfertigt
§ 206 StGB („Anvertrauen“)	Nicht anvertraut	Nicht anvertraut
§ 303a StGB („Verfügungsbefugt“)	Kein Eingriff	Kein Eingriff
Nutzungsverhältnis	Auslegung: keine Pflicht zur Annahme	Auslegung: keine Pflicht zur Annahme
Mitbestimmungsrecht Personalrat	Nein, da keine Überwachung möglich	Nein, da keine weitergehende Überwachung möglich
Information des Versender-Servers	Erforderlich	Erforderlich

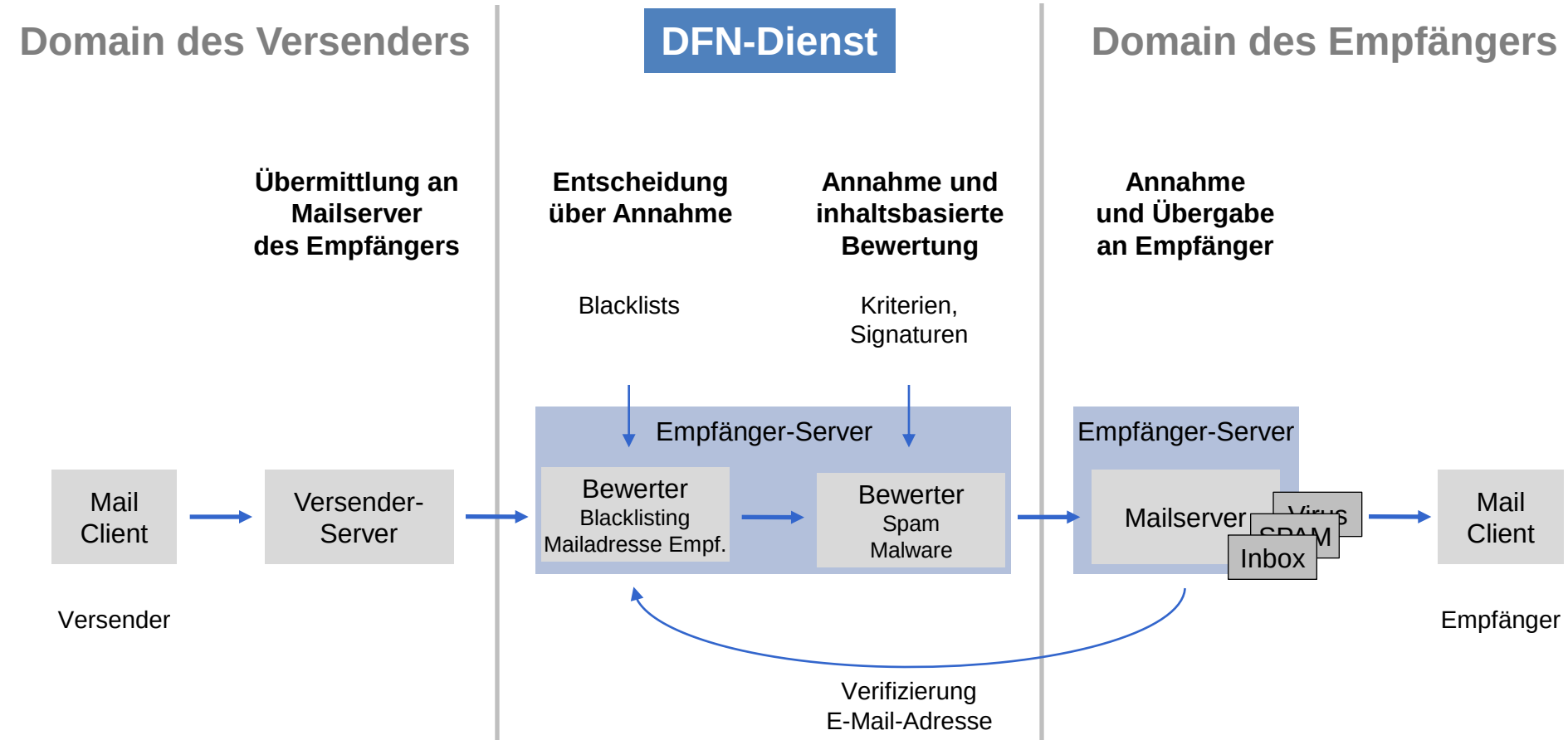
Technische Bewertung Blacklisting / Greylisting

- Blacklisting
  - ✓ setzt vor Übertragung des Inhalts der E-Mail ein
  - ✓ verarbeitet nur IP-Adressen von Versender-Servern
  - ! setzt Informationen von externen Quellen voraus
  - ✓ Verhalten in der Kontrolle des Empfänger-Servers
- Greylisting
  - ✓ setzt vor Übertragung des Inhalts der E-Mail ein
  - ! verarbeitet IP-Adressen von Versender-Servern sowie E-Mail-Adressen von Versender und Empfänger
  - ✓ setzt keine externen Informationen voraus
  - ! hängt vom Wohlverhalten der Versender-Server ab

E-Mail-Transfer mit Filter (2)



DFN-Dienst zur Abwehr verseuchter E-Mails



Ausgangslage DFN-Dienst

- Von allen Anwendern nutzbarer Dienst im Wissenschaftsnetz zur Abwehr von mit Spam oder Malware verseuchten E-Mails

- Ziele
  - Steigerung des allgemeinen Sicherheitsniveaus im Wissenschaftsnetz
  - Entlastung der lokalen E-Mail-Dienste

- Betrieb des lokalen E-Mail-Service durch Anwender weiterhin erforderlich!

Maßstäbe für Qualität

- Vertraulichkeit und Integrität
- Verfügbarkeit
- Zuverlässige Erkennung
- Rechtliche Absicherung

Implementierung

- Grundsätze
  - maximaler Schutz vor Angriffen und Kompromittierung
  - kein Verlust von E-Mails
  - kein dauerhaftes Speichern von E-Mails

- Folgerungen
  - Kontrolle des Dienstes durch hohe Fertigungstiefe
  - aber kommerzielle Komponenten wo notwendig
  - intensive Überwachung durch DFN-NOC und DFN-CERT

Durch DFN-Verein beherrschte Betriebsumgebung

Weitere Planung

- Betriebsaufnahme Anfang 2012

- als Bestandteil des Dienstes DFNInternet
  - d. h. Nutzung ohne separates Entgelt

- erste Produktivsysteme ab August 2011 verfügbar
  - Pilotbetrieb mit ersten Anwendern
  - Ziel ist Kontrolle und Optimierung des Dienstes im frühen Dialog mit den Anwendern

Fragen ...?