Fachhochschule Gelsenkirchen

Sicherheit von E-Mails
→ Ist die Spam-Flut zu stoppen?

Prof. Dr. Norbert Pohlmann

Institut für Internet-Sicherheit
Fachhochschule Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

Inhalt

- **E-Mail Anwendung und Spam**
- **Umfrage „E-Mail Verlässlichkeit“**
- **IP Reputation Service**
- **Zusammenfassung**

E-Mail Anwendung
→ Übersicht

- E-Mail ist eine **elastische Anwendung,** in der diskrete Medien, die zeitunabhängig sind, wie Text und Grafik, ausgetauscht werden.
- Der E-Mail Verkehr macht **12% der Bandbreite** im Backbone international agierender IP-Carrier aus.
- Pro Monat werden **mehrere Billion (10^{12}) E-Mails** weltweit ausgetauscht (120 Mrd./Tag; 3.6 Billionen/Monat; 2007).
- Obwohl die **E-Mail (SMTP) nicht als verlässlicher Dienst entworfen wurde**, dient die E-Mail-Anwendung heute der unkomplizierten und schnellen Kommunikation zwischen Geschäftspartnern und Privatleuten weltweit.
- **Spam**, **Viren** und **andere Schwachstellen** sind ein ernsthaftes Problem mit hohem Schaden und stellen **ein sehr hohes Sicherheitsrisiko dar!**
- **Dieser Trend lässt die Frage zu: Kann der E-Mail-Dienst in der nahen Zukunft noch genauso einfach und effizient eingesetzt werden wie bisher?**

E-Mail Anwendung
→ Definition: Spam

- Spam-Mails sind **unerwünschte, für den Empfänger wert-, nutz- oder sinnlose E-Mails**

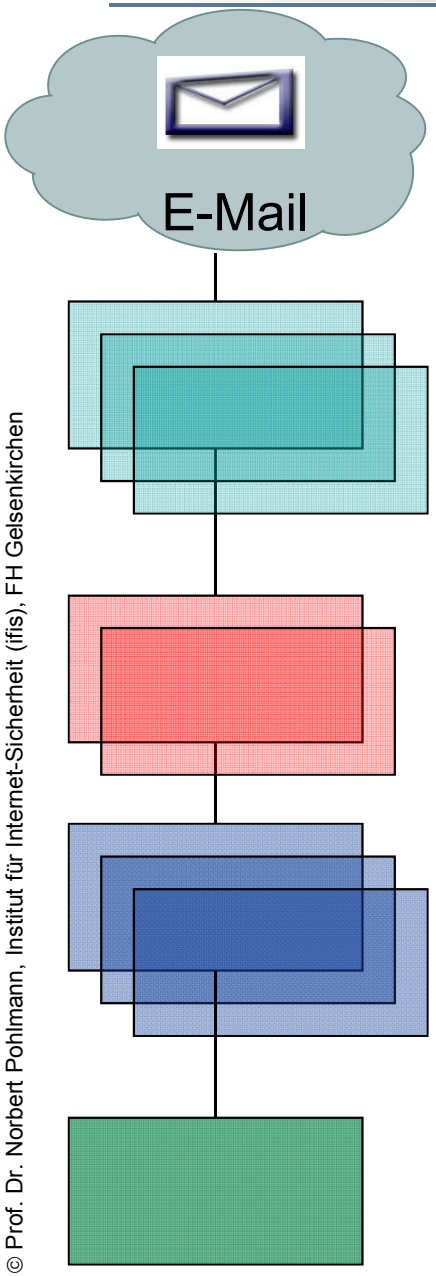
- **„Unerwünscht“ ist individuell …**
  - 92% bezeichnen unerwünschte Werbung als Spam
  - Werbung von politischen Gruppen oder Bürgervertretung: 74%
  - ... von Nonprofit- oder Wohltätigkeitsorganisationen nur noch 65%

- **aber: Spam-Nachrichten haben gemeinsam:**
  - Spam-Mails werden in Massen versendet
  - Es gibt einen geschäftlichen, politischen oder kriminellen Hintergrund

E-Mail Anwendung
→ Schäden, die durch Spam-Mails auftreten

- **Arbeitszeitverlust**
  (Echtzeitsignalisierung, erkennen, aussortieren und löschen)
- **Sicherheitsproblem**
  (Viren, Würmer, Trojaner)
- **Speichergebrauch**
  (Von nicht gewünschten Werbe-Mails)
- **Bandbreitenverbrauch**
  (Von nicht gewünschten Werbe-Mails)
- **Mail-Server Lahmlegung**
  (Rücklauf von fremden Spam-Mails)
- **Reputation des Betreibers**
  (Spammer nutzen andere Mail-Server - Pornographie, Gewalt, usw.)
- **Kosten für Anti-Spam-Maßnahmen**
  (Spam-Filter, IP-Reputation-Dienst, usw.)
- **Nutzbarkeit**
  (E-Mail ist wegen der sehr hohen Belastung nicht mehr nutzbar)

Anti-Spam-Techniken
→ Das Ebenen-Modell



Ext. E-Mail-Gateway / E-Mail-Proxy als Teil einer Firewall

- Checks auf IP-Ebene (IP-Adresse)
  - Blacklists (RBLs, Dynamische-/Dial-Up-IP, open relay, ...)
  - Reverse MX
  - Frequenzmessung
- Checks auf SMTP-Ebene
  - Überprüfen der HELO-Angabe
  - Überprüfen der Absender-E-Mail-Adresse (Black-/White-/Greylist)
  - Existenz der Empfänger-E-Mail-Adresse (DB, Verzeichnisdienst)

1

Spam-Filter

- Checks auf Header- und Nachrichten-Ebene
  - Header Checks, Wortliste,
  - Hash/Signatur
  - Body-Checks (Strings)

2

Viren-Filter

- Check Nachricht und Anhänge auf Virenbefall

3

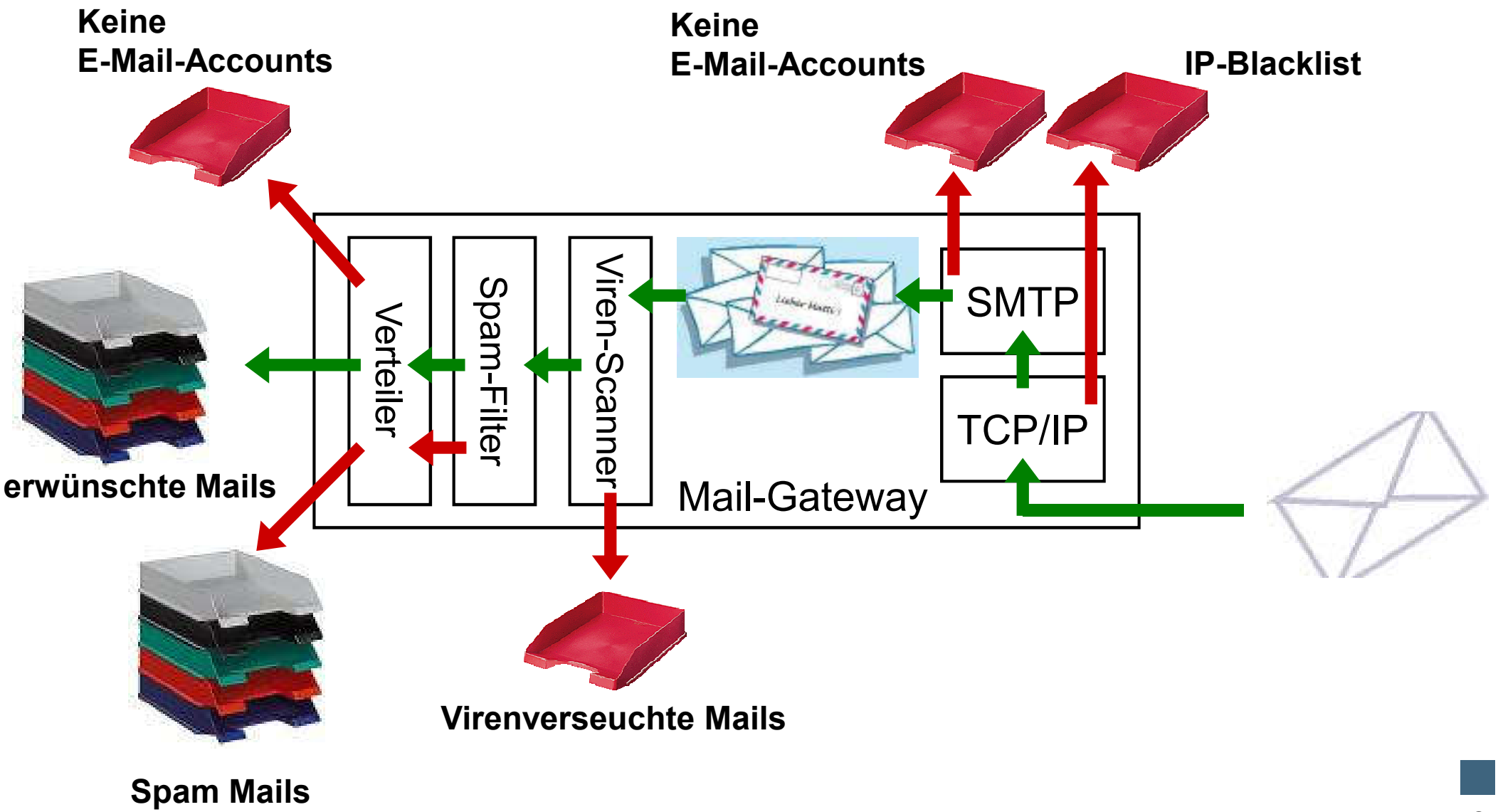
Ressourcenverbrauch

Interner E-Mail-Server

Inhalt

- E-Mail Anwendung
- **Umfrage „E-Mail Verlässlichkeit“**
- IP Reputation Service
- Zusammenfassung

Generalisierte Sichtweise
→ Übersicht über Maßnahmen

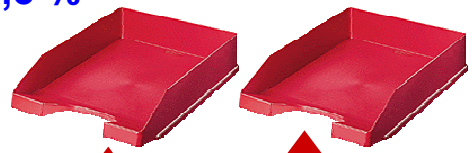


Generalisierte Sichtweise – Vergleich
→ Ergebnisse: System, Eingang

Keine
E-Mail-Accounts
10,24 % | 5,0 %* | 6,1 %**

Keine
E-Mail-Accounts
5,5 % | 11,7 %* | 2,5 %**

IP-Blacklist
3,03 % | 13,4 %* | 34,2 %**



erwünschte Mails
22,32% | 28,2%* | 18,8%**

Verteiler

Spam-Filter

Viren-Scanner

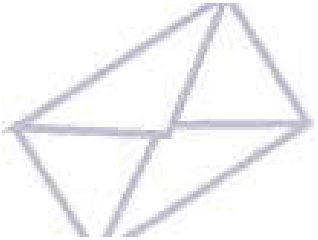
91,47 % | 74,9 %*
63,3 %**

SMTP

TCP/IP

Mail-Gateway

100 %



Spam Mails
56,26 % | 36,5 %* | 37,5 %**

Virenverseuchte Mails
2,65 % | 2,5 %* | 0,8 %**

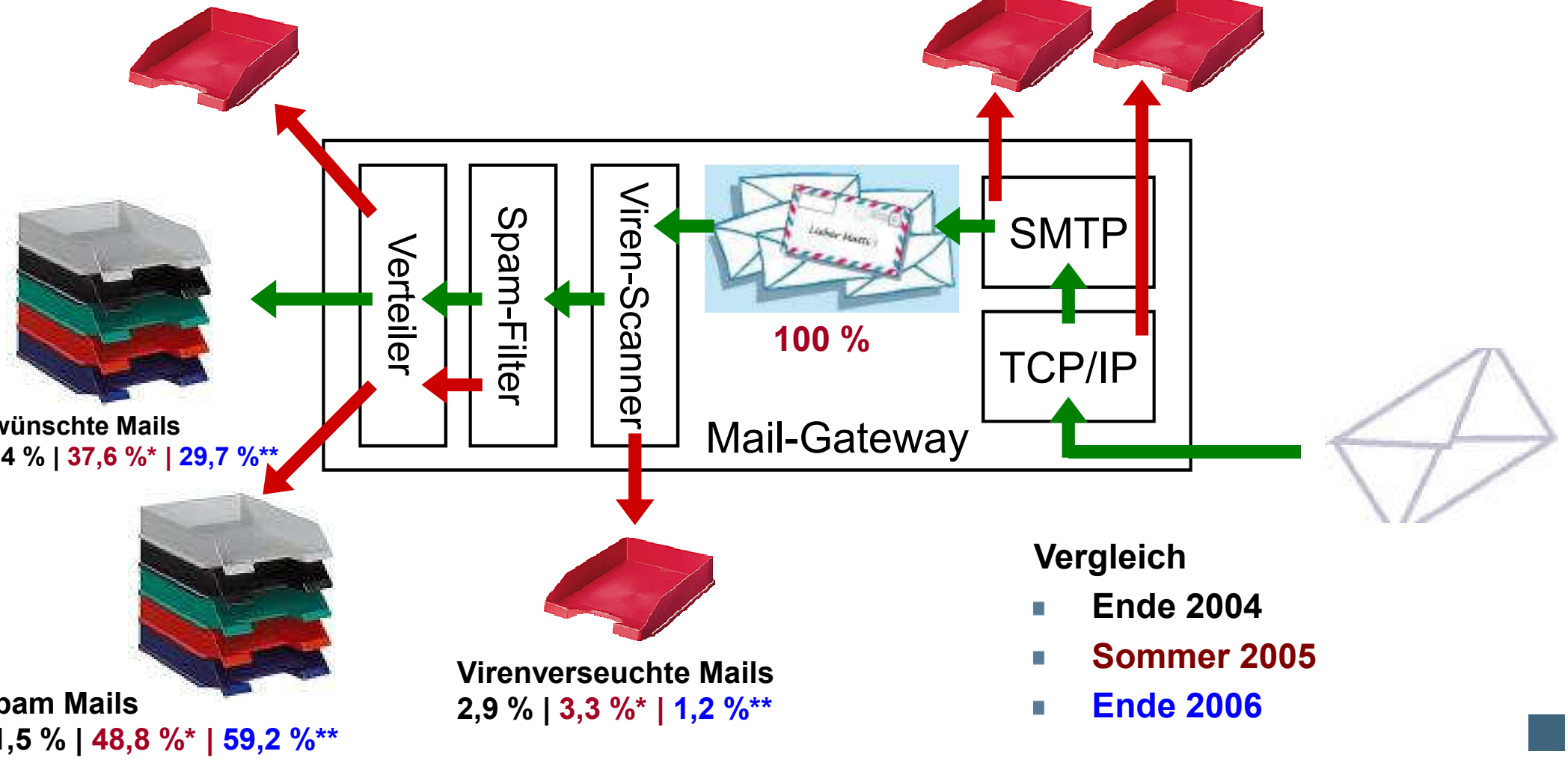
Vergleich

- **Ende 2004**
- **Sommer 2005**
- **Ende 2006**

*restliche 2,7 % nicht zuordbar

**restliche 0,4 % nicht zuordbar

Generalisierte Sichtweise – Vergleich → Ergebnisse: System, angenommene

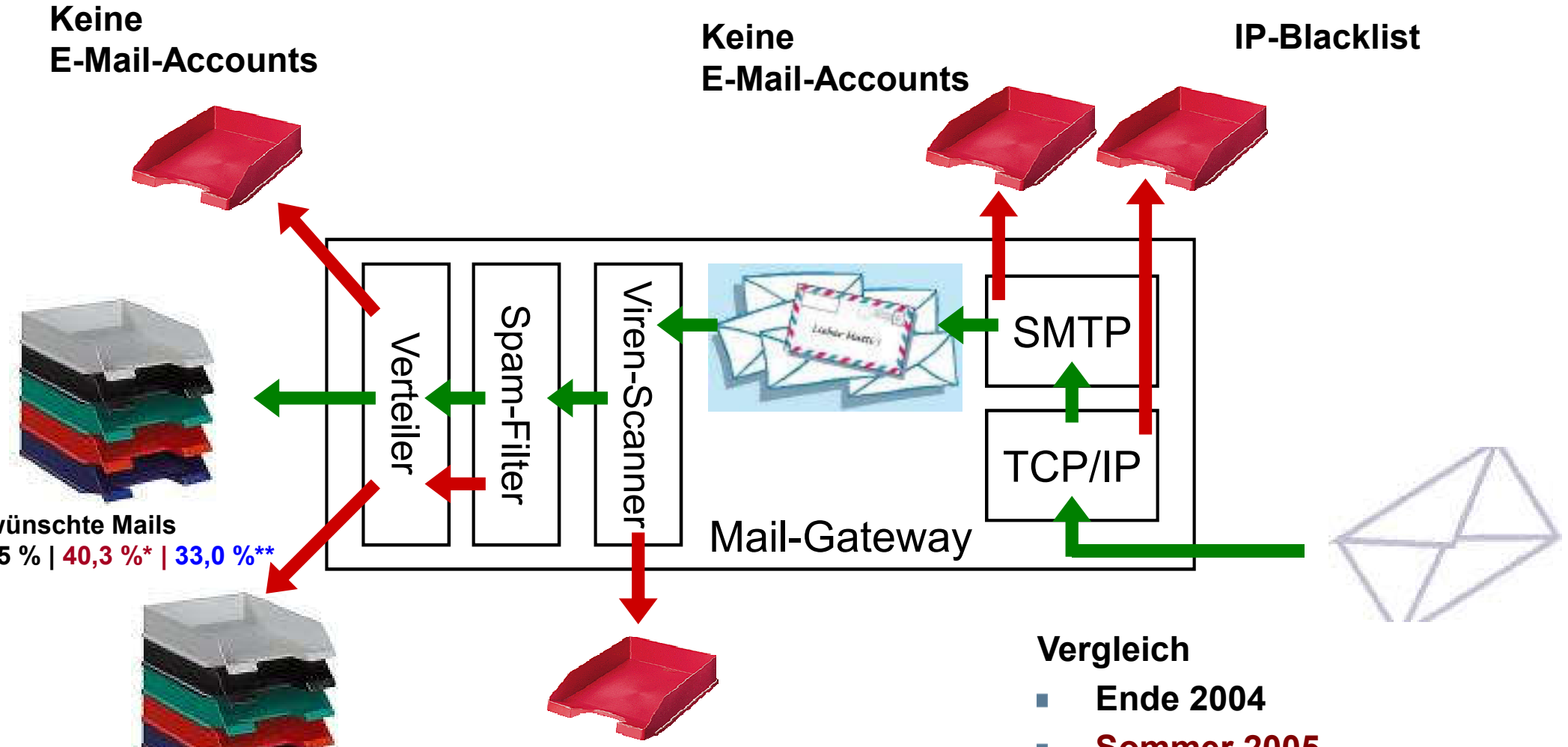


Vergleich

- Ende 2004
- Sommer 2005
- Ende 2006

*restliche 3,6 % nicht zuordbar **restliche 0,2 % nicht zuordbar

Generalisierte Sichtweise – Vergleich
→ Ergebnisse: Nutzerperspektive

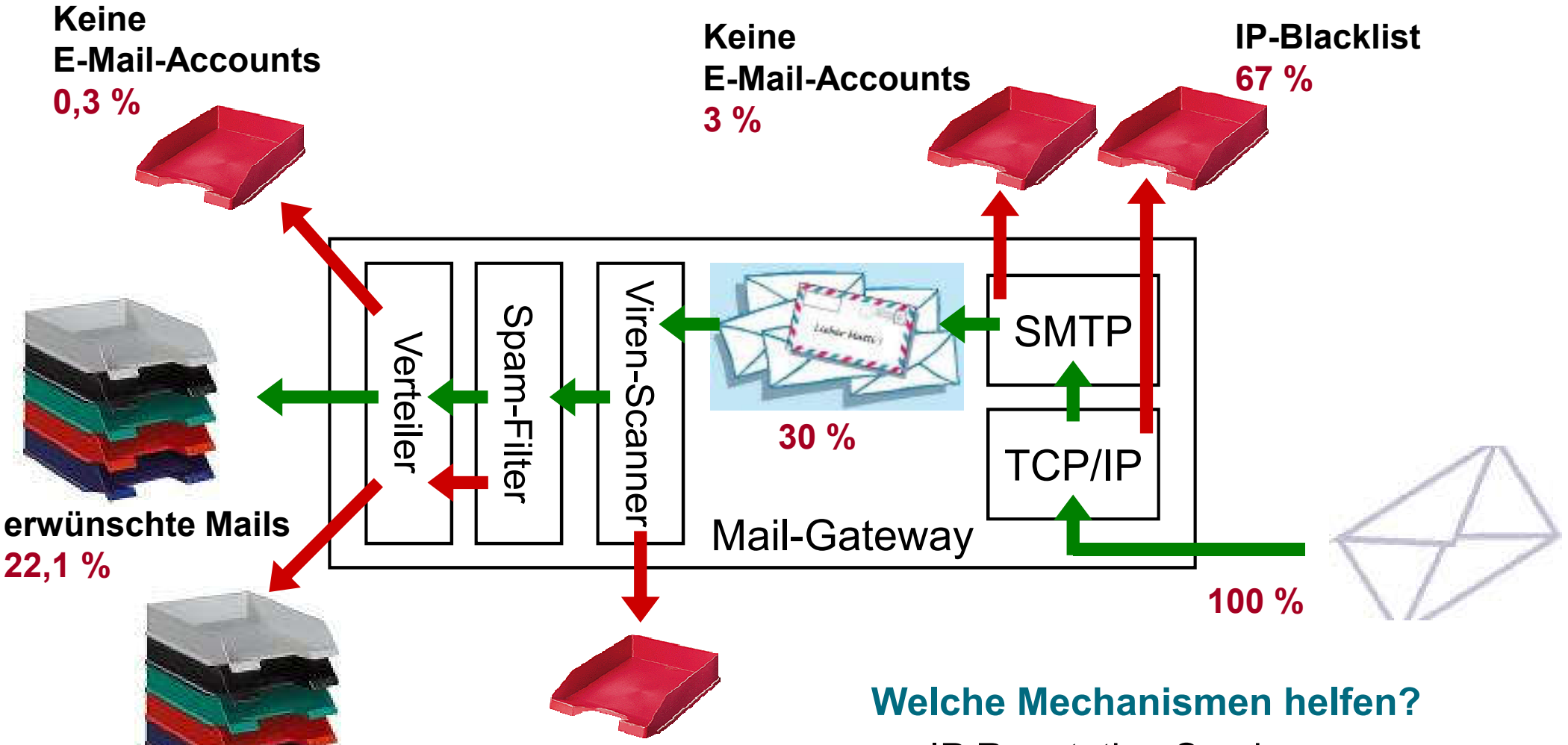


Vergleich

- Ende 2004
- Sommer 2005
- Ende 2006

*restliche 3,9 % nicht zuordbar **restliche 0,1 % nicht zuordbar

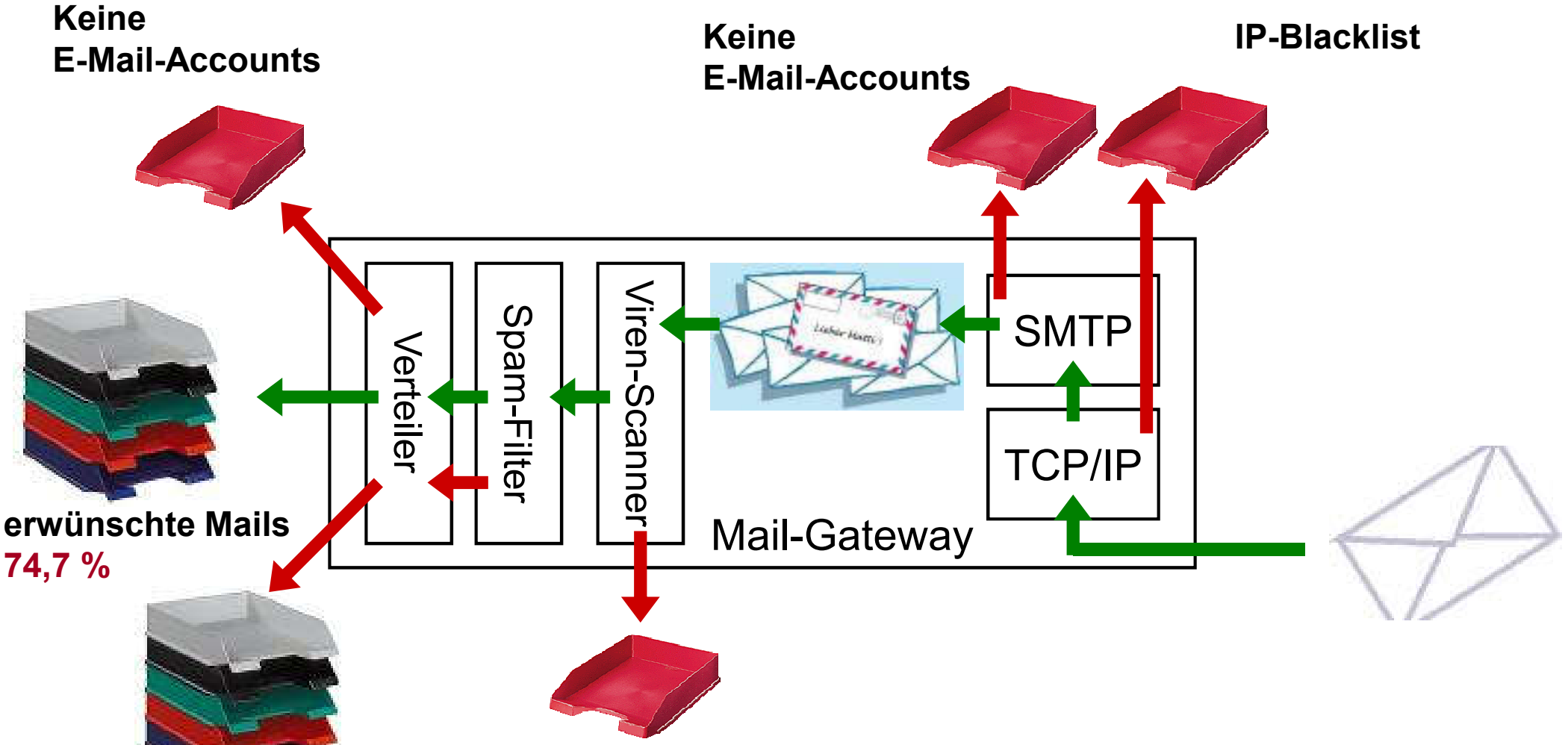
E-Mail Verlässlichkeit
→ Ideen/Empfehlungen: System, Eingang



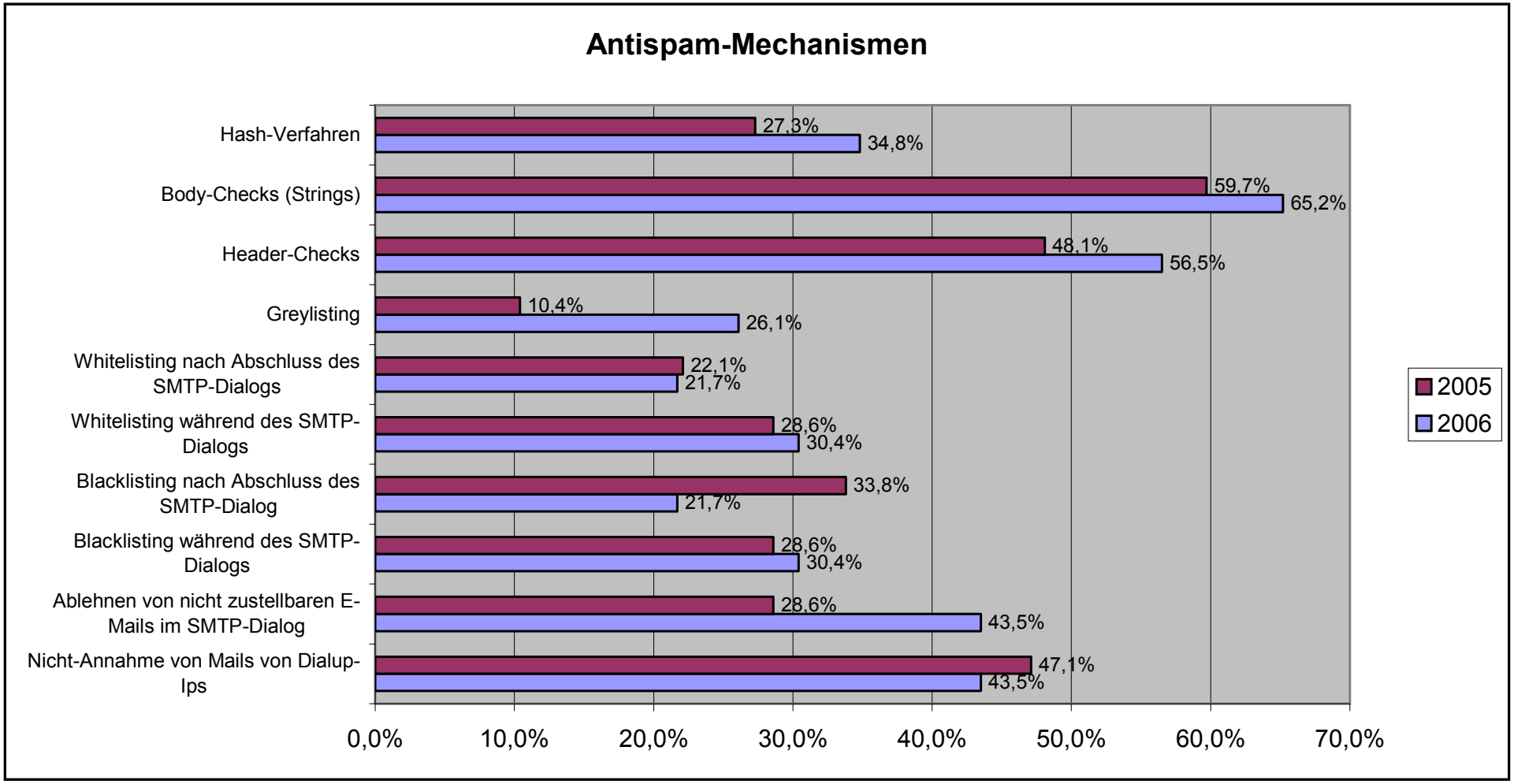
Welche Mechanismen helfen?

- IP Reputation Service
- Vor der Annahme prüfen, ob ein E-Mail-Account vorhanden ist

E-Mail Verlässlichkeit
→ Ideen/Empfehl.: Nutzerperspektive



Antispam-Mechanismen (Verbreitung) → (Vergleich: 1. und 3. Lauf)



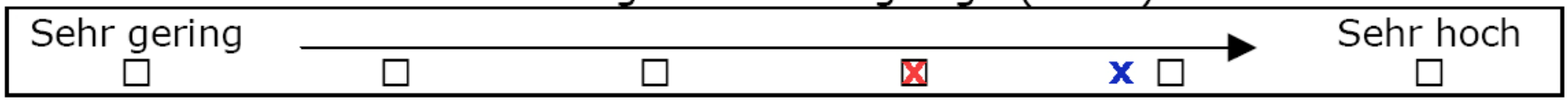
- **Zunahme:** Greylisting, Hash-Verfahren, Header-Checks, Ablehnen von nicht-zustellbaren E-Mails im SMTP-Dialog
- **Abnahme:** **Nicht-Annahme von Dialup-IPs (!),** Black- und Whitelisting nach Abschluss des SMTP-Dialogs (hoher Aufwand!)

Key Findings

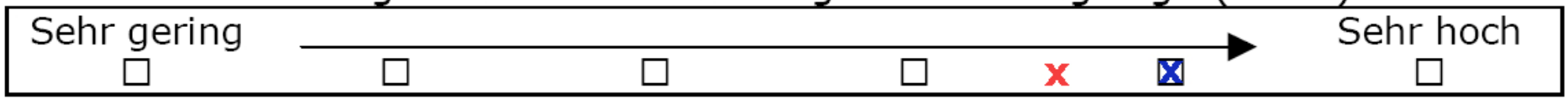
Lauf	1 (Ende 04)	2 (Sommer 05)	3 (Ende 06)	
Erwünschte Mails	**22,32**	**28,2**	**18,8**	↓
Viren	**2,65**	**2,5**	**0,8**	↓
Spam (Rest)	**75,03**	**69,3**	**80,4**	↑
Verschlüsselte Mails	4,3		2,2 (9,2)	↓
Signierte Mails	5,9		4 (10,8)	↓
Kein Spam-Schutz	8,9		9	→
kritische Geschäftsp.	**45**		**66**	↑

E-Mail Verlässlichkeit
→ Einschätzung der Bedrohungslage

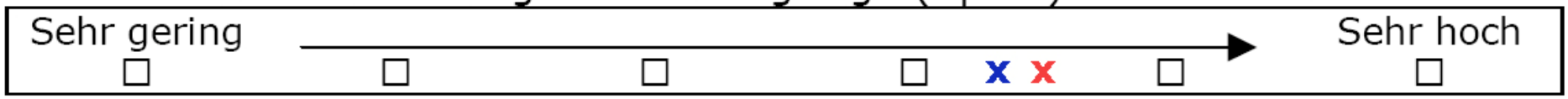
30. Wie würden Sie die heutige Bedrohungslage (Viren) einschätzen?



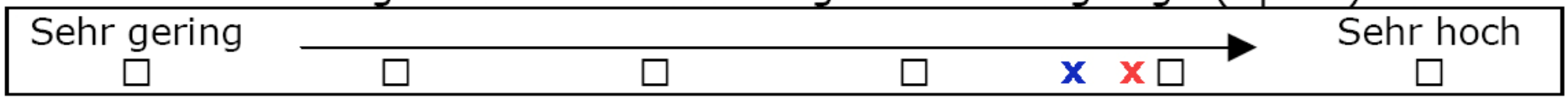
Wie sieht Ihre Prognose für die zukünftige Bedrohungslage (Viren) aus?



Wie würden Sie die heutige Bedrohungslage (Spam) einschätzen?



Wie sieht Ihre Prognose für die zukünftige Bedrohungslage (Spam) aus?



x 2004 x 2006

- **Spam wird im Vergleich zu Viren als die größere Gefahr wahrgenommen (neu!).**

Inhalt

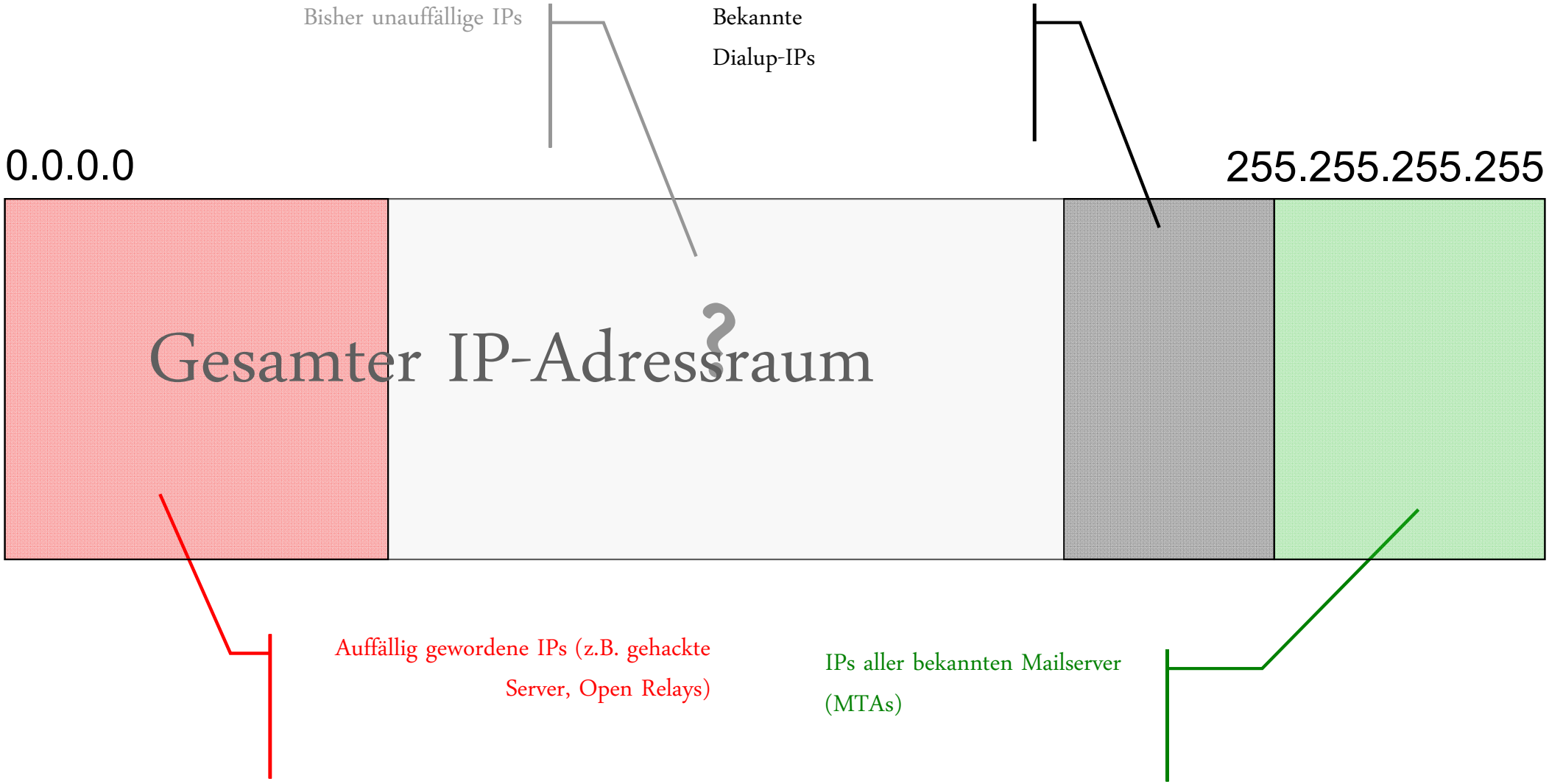
- E-Mail Anwendung
- Umfrage „E-Mail Verlässlichkeit“
- **IP Reputation Service**
- Zusammenfassung

IP Reputation Service
→ E-Mail

- **IP Reputation**
  - „Wertschätzung“ einer IP-Adresse
  - Dienst zur Abfrage einer dienstorientierten Qualität
  - Beispiel: E-Mail
    - Es wird ein deutlich erhöhter inbound SMTP-Traffic von der IP-Adr. 213.165.64.20 festgestellt
    - Mit dem Wissen, dass es sich bei der 213.165.64.20 um einen der Mailouts eines bekannten E-Mail-Provider handelt folgt
    - Vermutlich **legitimer Traffic** ➔ „Alles o.k.“

- **Nutzung eines IP Reputation Service**
  - Bei Aufbau der SMTP-Verbindung wird gefragt, welche Reputation die einliefernde IP-Adresse (E-Mail-Gateway, …) hat.
  - In der Regel DNS-basiert (sog. DNSBLs oder DNS Blacklist)
  - Wenn die Reputation passt, dann Annahme der E-Mail, sonst Ablehnung der E-Mail im SMTP-Dialog.

Grundsätzliche Idee
→ Die „IP-Karte“

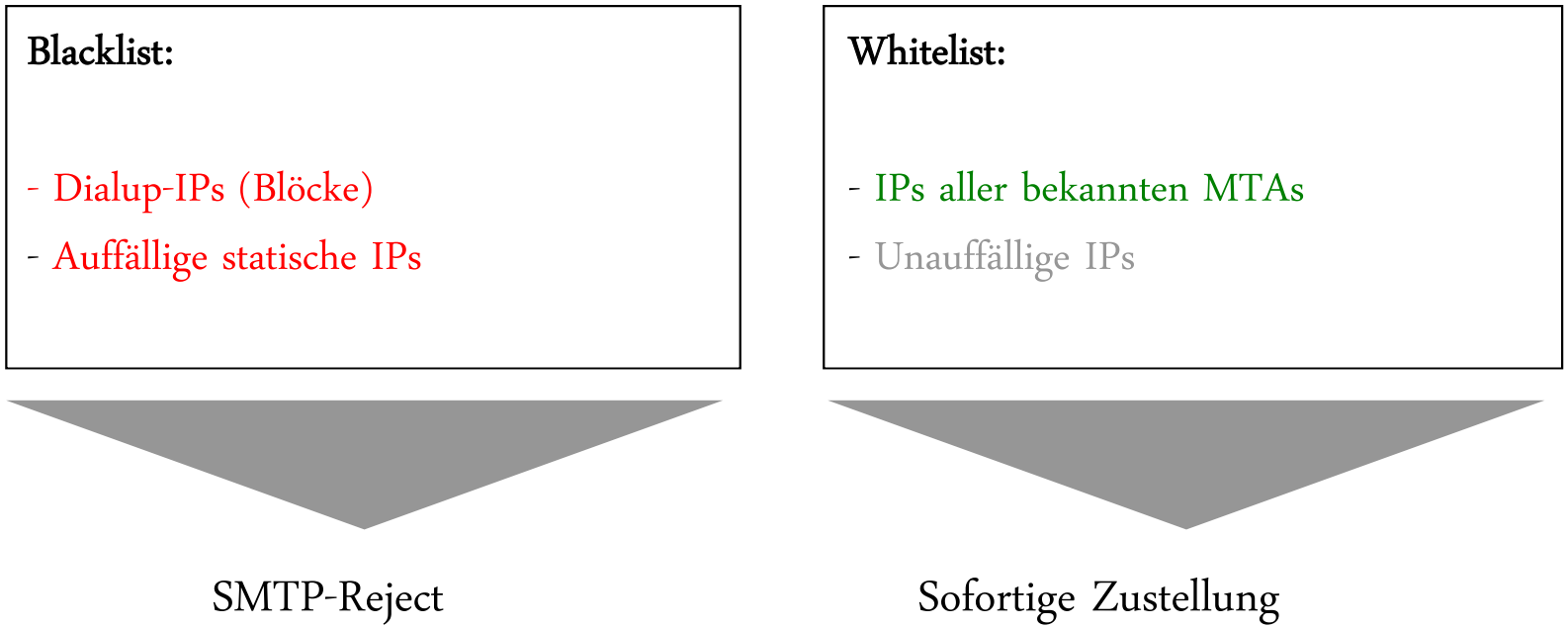


Aktuelles Vorgehen bei ISPs
→ Systematik einer IP-Karte

- Die hinterlegten bekannten E-Mail-Server sowie die Dialup-IP-Blöcke beruhen auf Beobachtung der ISP-Landschaft.
- IP-Verbindungen von unbekannten bzw. bisher unauffälligen IPs werden zugelassen, d.h. die Mails werden angenommen.
- Eine Eintragung in die Blacklist ist abhängig vom Vorliegen konkreten Spam-Verdachts (Beschwerden, Zahl der Mails, Anteil gültiger Adressen, etc.)

Aktuelles Vorgehen bei ISPs
→ Black- & Whitelist

- Die dargestellte „IP-Karte“ ist Basis für die manuelle Erstellung einer Blacklist bzw. Whitelist.

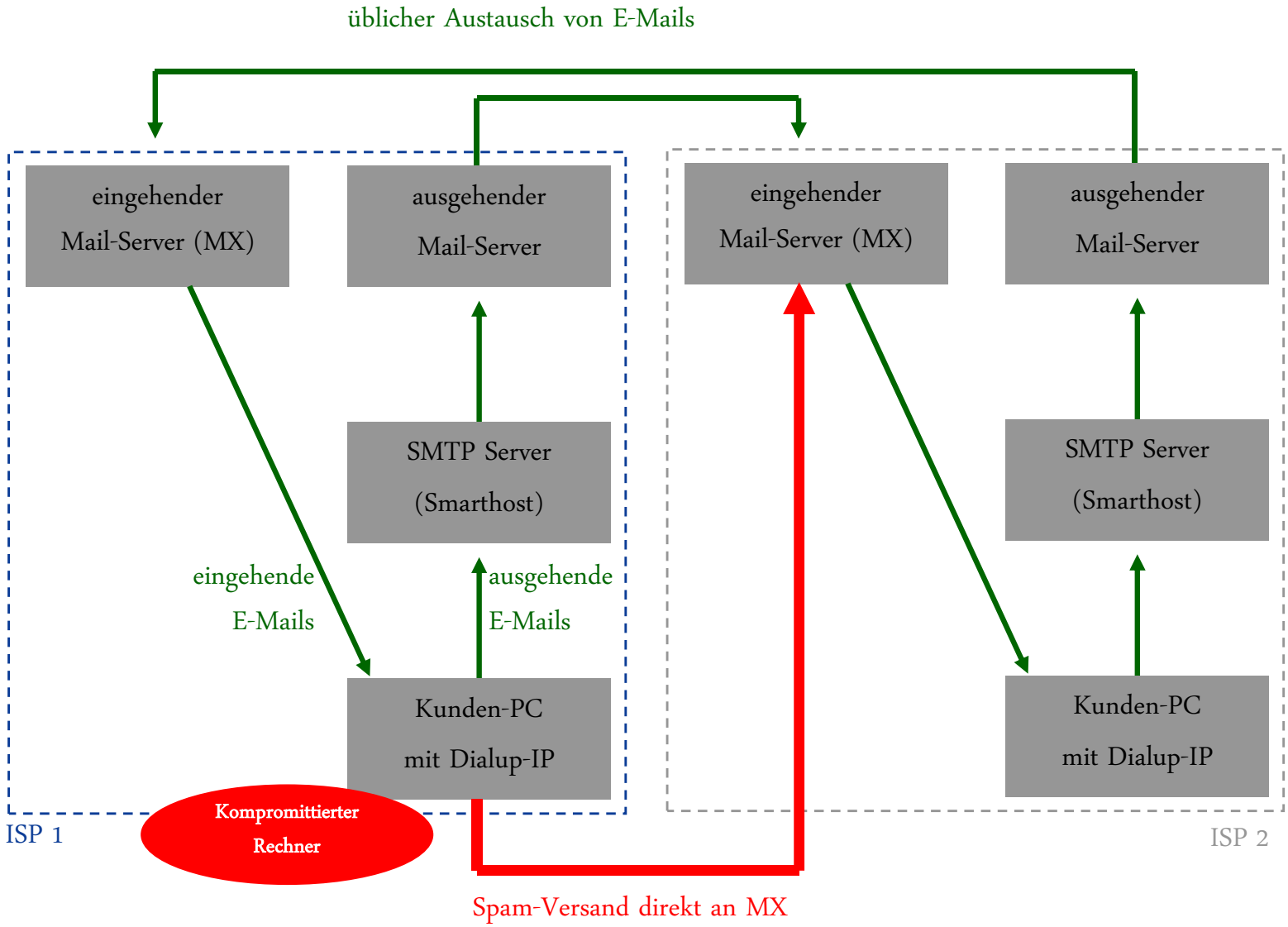


Dialup-IPs sind Spam-Quelle Nr. 1
→ Bot-Viren und Spam

- 67% des Spam-Aufkommens wird durch sogenannte „Bot-Viren“ verursacht, die PCs befallen.
- „Bot-Viren“ versenden massenhaft Spam-Mails direkt an die eingehenden Mail-Server der jeweiligen E-Mail-Provider
- Smarthosts der Provider werden umgangen
- PCs erhalten bei jeder Einwahl eine dynamische Dialup-IP aus dem IP-Nummernblock des jeweiligen ISPs zugewiesen

- **Feststellung**
  - **Dialup-IPs versenden niemals erwünschte E-Mails an eingehende Mail-Server**
  - **Sie zu blocken hat keinen großen Nachteil!**

Dialup-IPs sind Spam-Quelle Nr. 1
→ Spam-Versand direkt an MX



Aktuelles Vorgehen bei ISPs
→ Potenzial einer IP-Karte

- **Die Rate** der erkannten Spam-Mails muss und kann noch weiter **gesteigert werden**.
- Hierzu müssen Spam-IPs vor allem **schneller identifiziert werden** als heute.
- Eine **„IP-Karte“** muss national bzw. **global etabliert werden**, um Spam-Mails generell und nachhaltig einzudämmen.

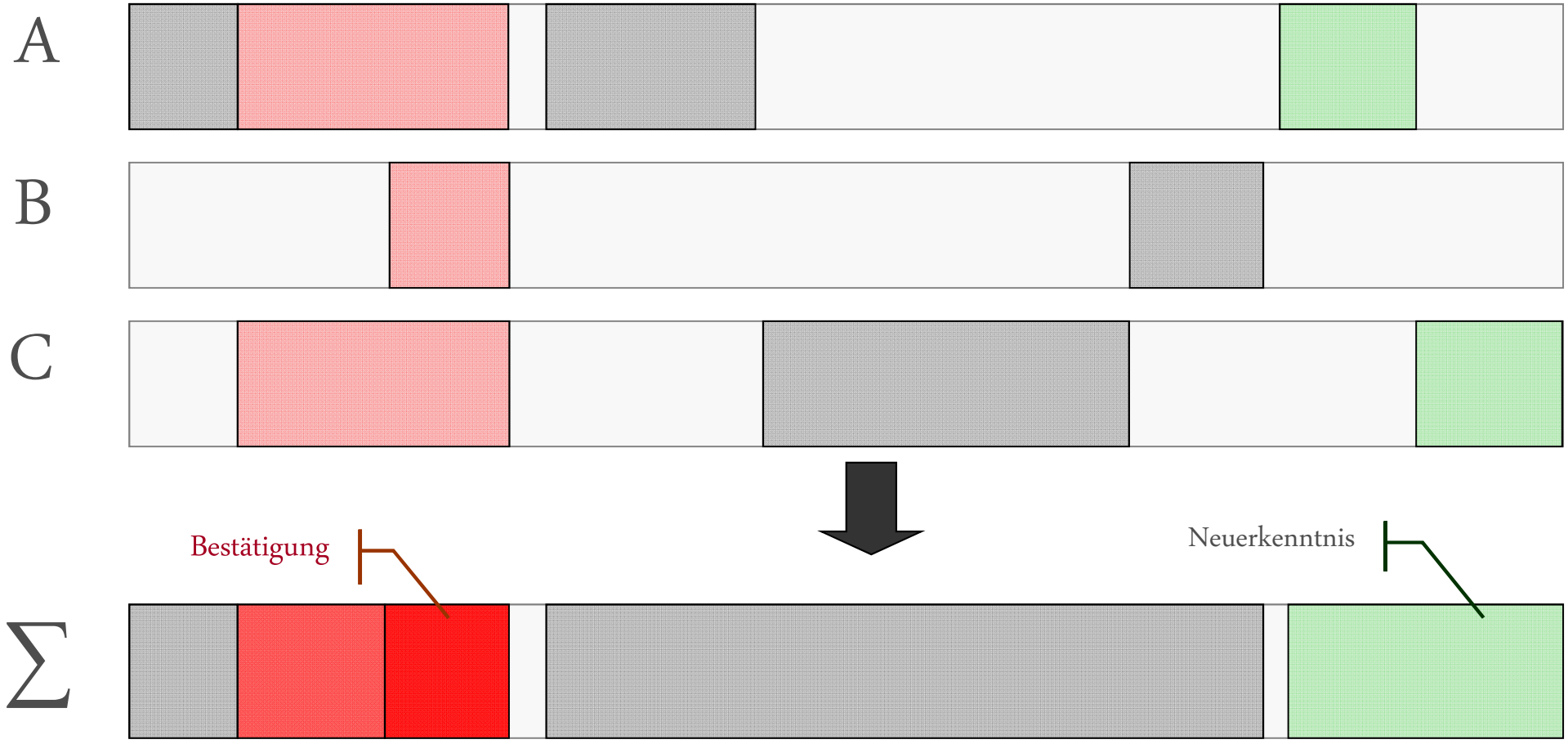
- **Notwendiges Vorgehen:**
  - **Austausch von „IP-Karten“ und Selbstauskünften zwischen interessierten ISPs weltweit!**

Konzept einer globalen Lösung
→ Selbstauskunft und „Spam-Karte“

- Die **ISPs** tauschen regelmäßig Selbstauskünfte und Beobachtungsdaten (**„IP-Karten“**) aus.
- Es handelt sich dabei um **attributierte IP-Listen**.
- Diese enthalten auch die AS-Nummern, um die **Überprüfbarkeit der Angaben** sicherzustellen.

Selbstauskunft	„Spam-Karte“
- IPs aller Mailserver (MTAs) - Dialup-IPs (Blöcke) evtl. zusätzlich: - statisch vergebene IPs	- Auffällige IPs - IPs schlecht administrierter Mailserver (MTAs)

Konzept einer globalen Lösung
→ Interpretation der „IP-Karten“



- Ein Abgleich, mit Hilfe eines **adaptiven Vertrauensmechanismus**, der Reputation **bestätigt** oder **relativiert** eigene Beobachtungen und **zeigt neue potentielle Spam-Quellen** auf.

Konzept einer globalen Lösung
→ Vorteile einer IP-Karte

- Im Sinne einer **Semi-Closed-User-Group** steht die IP-Karte prinzipiell allen ISPs offen.
- Bereits mit wenigen aktiven Teilnehmern der IP-Karte ist eine hohe Abdeckung der auffälligen IP-Adressen und damit eine schnelle und **wirksame Spam-Identifikation** zu erreichen.
- Die **Selbstauskünfte** der aktiven ISPs **verringern** das Risiko von **„false positive“ Fällen**.
- Jeder Teilnehmer ist frei in der Verwendung der aus dem Austausch gewonnen Informationen (adaptiver Vertrauensmechanismus).
- **Dezentrale Struktur** verhindert Mißbrauch durch einzelne Teilnehmer und **erhöht die Verfügbarkeit** des IP Reputation Services.

Ist die Spam-Flut zu stoppen?
→ Zusammenfassung

- **Spam-Mails sind ein komplexes Problem des globalen Internets.**

- Pragmatische Anti-Spam Produkte und Lösungen auf der Ebene 2 (Modell), helfen uns, mit der Spam-Flut umzugehen (markieren, in spezielle Ordner verschieben, usw.)

- **Neue IP Reputation Services Konzepte werden helfen, das Spam-Problem deutlich zu reduzieren und damit Schäden zu vermeiden**
  - Eine **internationale Zusammenarbeit** ist **besonders effektiv**
  - **Frequenzanalysen** des Kommunikationsverhaltens der E-Mail-Partner und weitere Validierungen helfen, Reputationen von IP-Adressen zu bekommen und zu optimieren

- **Weitere Informationen unter: www.internet-sicherheit.de**

Fachhochschule Gelsenkirchen

Sicherheit von E-Mails
→ Ist die Spam-Flut zu stoppen?

Vielen Dank für Ihre Aufmerksamkeit
Fragen ?

Prof. Dr. Norbert Pohlmann

Institut für Internet-Sicherheit
Fachhochschule Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.