

Kein Platz für Spams und Viren – Lösungsbeispiele zum wirksamen Schutz vor der Gefahr der Online-Kommunikation

Prof. Dr. Norbert Pohlmann

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

- **E-Mail Anwendung**
- **Umfrage „E-Mail Verlässlichkeit“**
- **Einschätzung „Viren, Würmer, Trojaner, ...“**
- **Einschätzung „Spam“**
- **Digitale Signatur und Verschlüsselung
(Passwort Fishing)**
- **Zusammenfassung**

- **E-Mail Anwendung**
 - Umfrage „E-Mail Verlässlichkeit“
 - Einschätzung „Viren, Würmer, Trojaner, ...“
 - Einschätzung „Spam“
 - Digitale Signatur und Verschlüsselung
(Passwort Fishing)
 - Zusammenfassung

- E-Mail ist ein **textbasiertes Kommunikationswerkzeug**, mit dem weltweit einfach und schnell Informationen ausgetauscht werden können.
- E-Mail ist ein Ersatz für:
 - Die „Schneckenpost“: Postkarten, Briefe und Päckchen
 - Für Faxe
- E-Mail ist eine **elastische Anwendung**, in der diskrete Medien, die zeitunabhängig sind, wie Text und Grafik, ausgetauscht werden.
- Vorteile der E-Mail-Anwendung sind:
 - **Einfach** – jeder kann damit umgehen (Einfache Namen, Handhabung)
 - **Schnell** – innerhalb weniger Sekunden
 - **Weltweit** – jeder kann immer erreicht werden (Mail-Boxen)
 - **Kein Medienbruch** – die Info. können weiter verwendet werden
 - **Kostengünstig** – keine extra Kosten für den Transfer

E-Mail

→ Eine globale Herausforderung

- Echtzeit Business erfordert
 - **Sicherheit,**
 - **Vertrauen und**
 - **Verfügbarkeit**

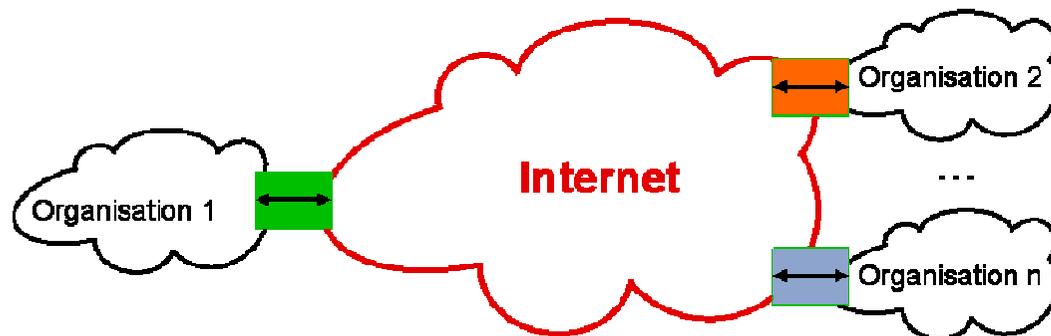
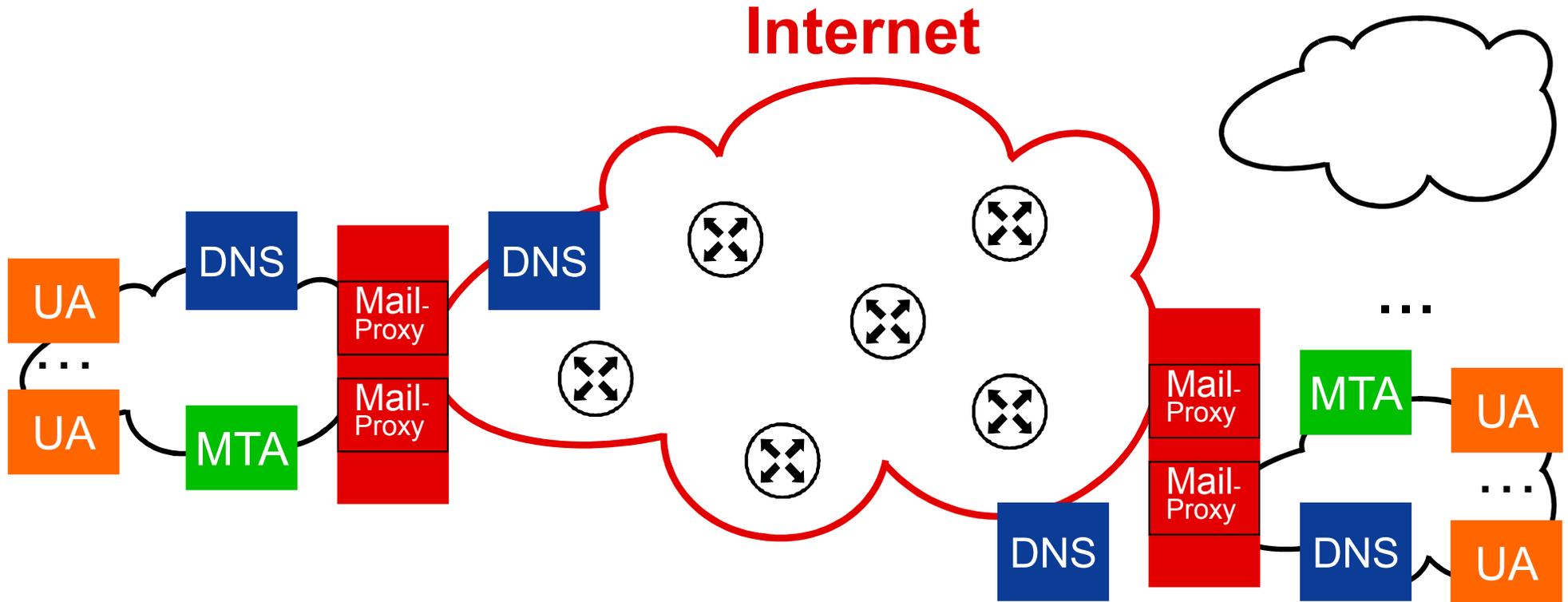
in allen gesellschaftlichen und wirtschaftlichen Bereichen!
- Das Internet geht über alle
 - **geographischen Grenzen,**
 - **politischen/administrativen Grenzen und**
 - **Kulturen hinaus**

und stellt somit eine neue und ungewohnte Herausforderung für die internationale Gesellschaft dar.
- Die Geschwindigkeit, in der **neue Anforderungen** auftauchen wird immer rasanter und damit **steigt das Sicherheitsrisiko.**

- E-Mail macht 12% der Bandbreite im Backbone international agierender IP-Carrier aus und ist die meistgenutzte Anwendung im Internet.
- Pro Monat ca. 900 Mrd. E-Mails weltweit.
- Obwohl die **E-Mail nicht als verlässlicher Dienst entworfen wurde**, dient die E-Mail-Anwendung heute der unkomplizierten und schnellen Kommunikation zwischen Geschäftspartnern und Privatleuten weltweit.
- Gerade aufgrund der geschäftlichen Nutzung wird dem E-Mail Dienst ein sehr **hohes Maß an Zuverlässigkeit abverlangt**.
- E-Mail im beruflichen Alltag
 - Zu viele E-Mails an einem Tag (mehr als 50 Stück)
 - Zu schnelle Reaktion (schlechte Qualität)
 - Disziplin beim Versenden (wichtig/unwichtig; AN/CC)
 - **Wir brauchen eine passende E-Mail-Kultur!**

E-Mail im globalen Internet

→ Beispiel eines Szenario (Unternehmen)



Notwendige Sicherheitsdienste: Gewährleistung der

- Vertraulichkeit
- Authentikation
- Integrität
- Verbindlichkeit
- Verfügbarkeit

E-Mail Anwendung

→ Wo liegen die Gefahren? (1/2)

- **Jeder kann uns E-Mails senden!**
 - Die, die wir wollen → **OK**
 - Die, die wir nicht wollen (Werbung, politische Inhalte, kriminelle Absichten, ...) → **Spam**
 - Die, die uns einen direkten Schaden zufügen sollen → **Viren, Würmer, Trojaner und Passwort Fishing**
- **Eine E-Mail ist wie eine Postkarte!**
 - Es wird keine Vertraulichkeit garantiert (siehe auch BlackBerry-Problematik)!
 - Kreditkartennummern und weitere Bankdaten, werden im Klartext übertragen!
- **Fehlende Nachweisbarkeit**
 - Absender der E-Mail, Echtheit des Inhaltes der E-Mail
 - Gewissheit, dass die E-Mail angekommen ist (Bestellungen, usw.)
 - Verbindlichkeit einer Bestellung (Zimmer, Tagungsräume, usw.)

E-Mail Anwendung

→ Wo liegen die Gefahren? (2/2)

- Auch wenn in der Regel alles funktioniert, die E-Mail-Anwendung stellt ein sehr hohes Sicherheitsrisiko dar!
- SPAM, Viren und andere Schwachstellen sind ein ernsthaftes Problem mit hohem Schaden und einem sehr hohen Schadenspotential.
- E-Mail ist für die Informationsgesellschaft und für den einzelnen ein nicht mehr wegzudenkender Service.

- E-Mail Anwendung
- **Umfrage „E-Mail Verlässlichkeit“**
- Einschätzung „Viren, Würmer, Trojaner, ...“
- Einschätzung „Spam“
- Digitale Signatur und Verschlüsselung
(Passwort Fishing)
- Zusammenfassung

Ziele der Umfrage

→ E-Mail Verlässlichkeit

- Feststellung bezüglich:
 - Der Art der Informationen, die per E-Mail ausgetauscht werden
 - Der Anteilsverteilung des E-Mail-Volumens (Spam, Viren und Co.)
 - Des aktuellen Bedrohungszustandes
 - Der eingesetzten Gegenmaßnahmen
 - Welche Aspekte sich über die Zeit verändern

Vollständige Auswertungen siehe: www.internet-sicherheit.de

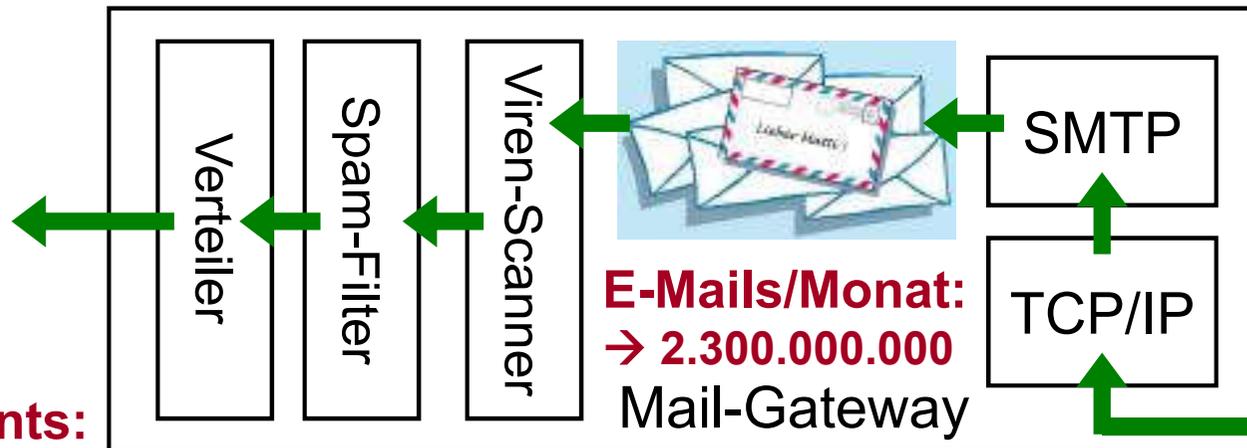
Allgemeine Statistik

→ Generalisierte Sichtweise



E-Mail-Accounts:
→ 40.000.000

- Pro **AG**
ca. 80 T E-Mail-Adressen
- Pro **GmbH**
ca. 3 T E-Mail-Adressen
- Pro **ISP**
ca. 5,5 Mio. E-Mail-Adressen



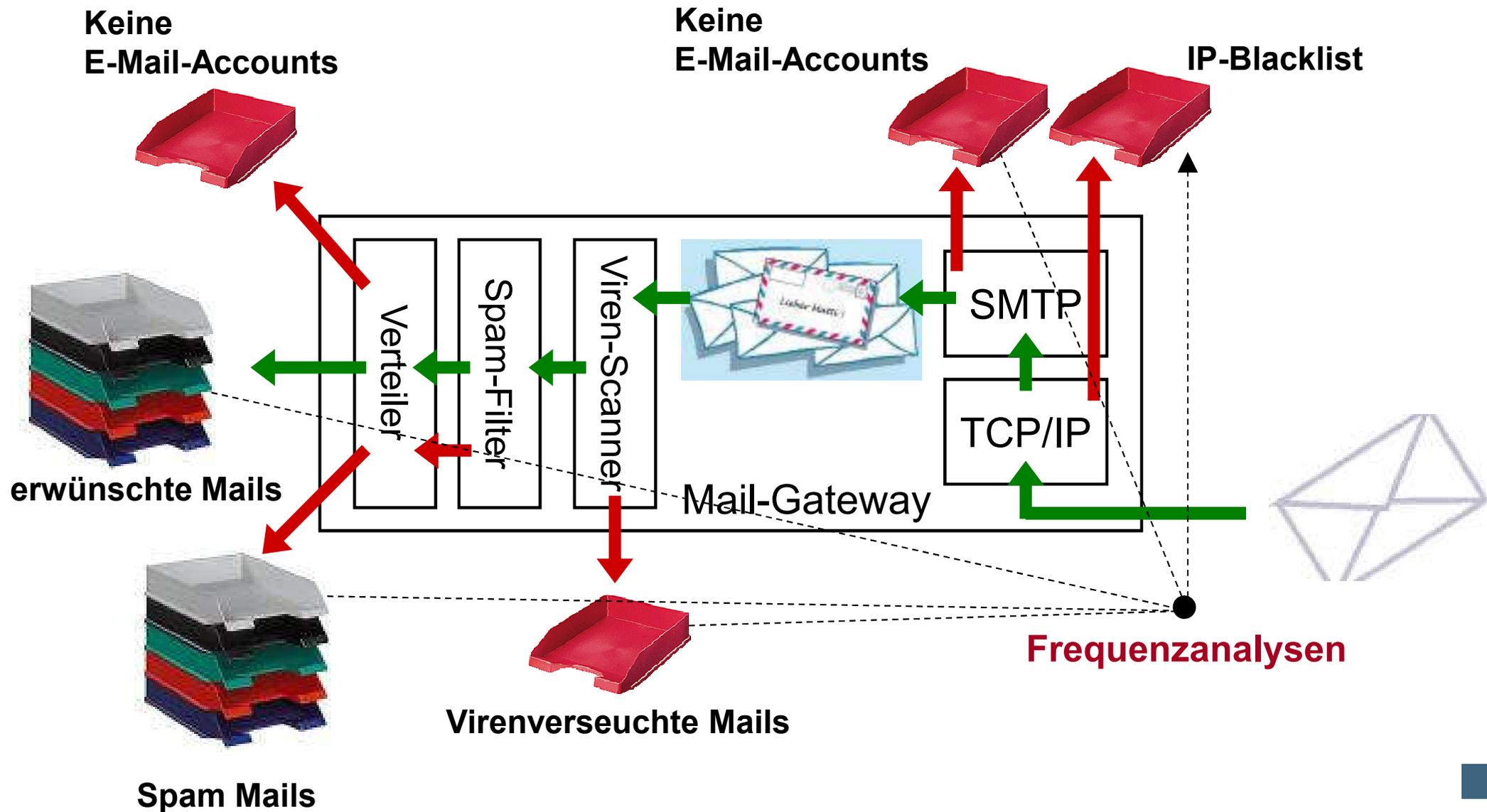
E-Mails/Monat:
→ 2.300.000.000

Teilnehmer:
→ 119

Rechtsform	
AG	13
Behörde	34
GmbH	28
Hochschule	9
ISP	7
Andere	28
Gesamt	119

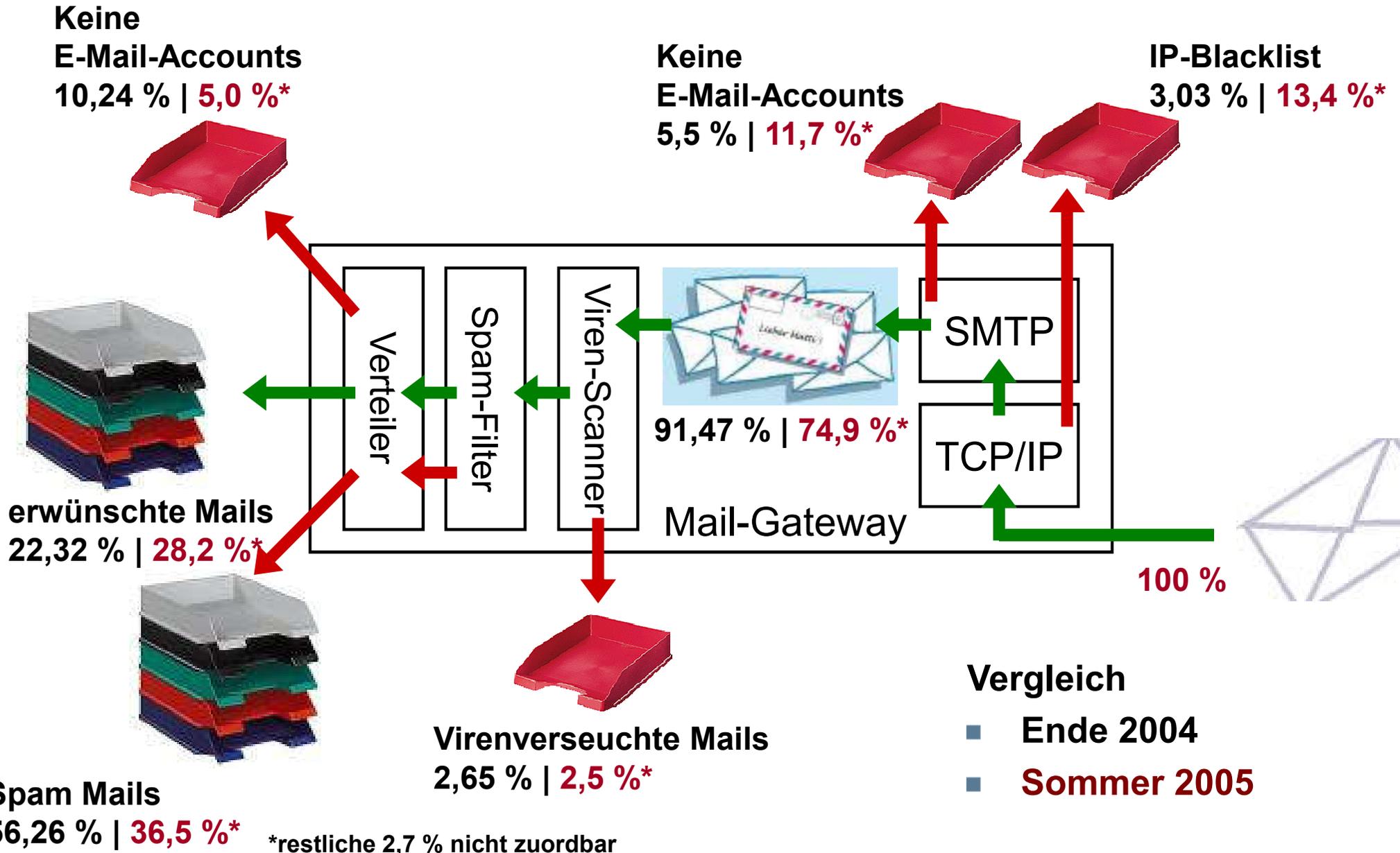
- Annahme 900 Mrd. E-Mails pro Monat weltweit
- **1/400 aller E-Mails weltweit**
- E-Mails über ISPs machen 91 % aller E-Mails dieser Umfrage aus

Generalisierte Sichtweise → Übersicht über Maßnahmen



Generalisierte Sichtweise – Vergleich

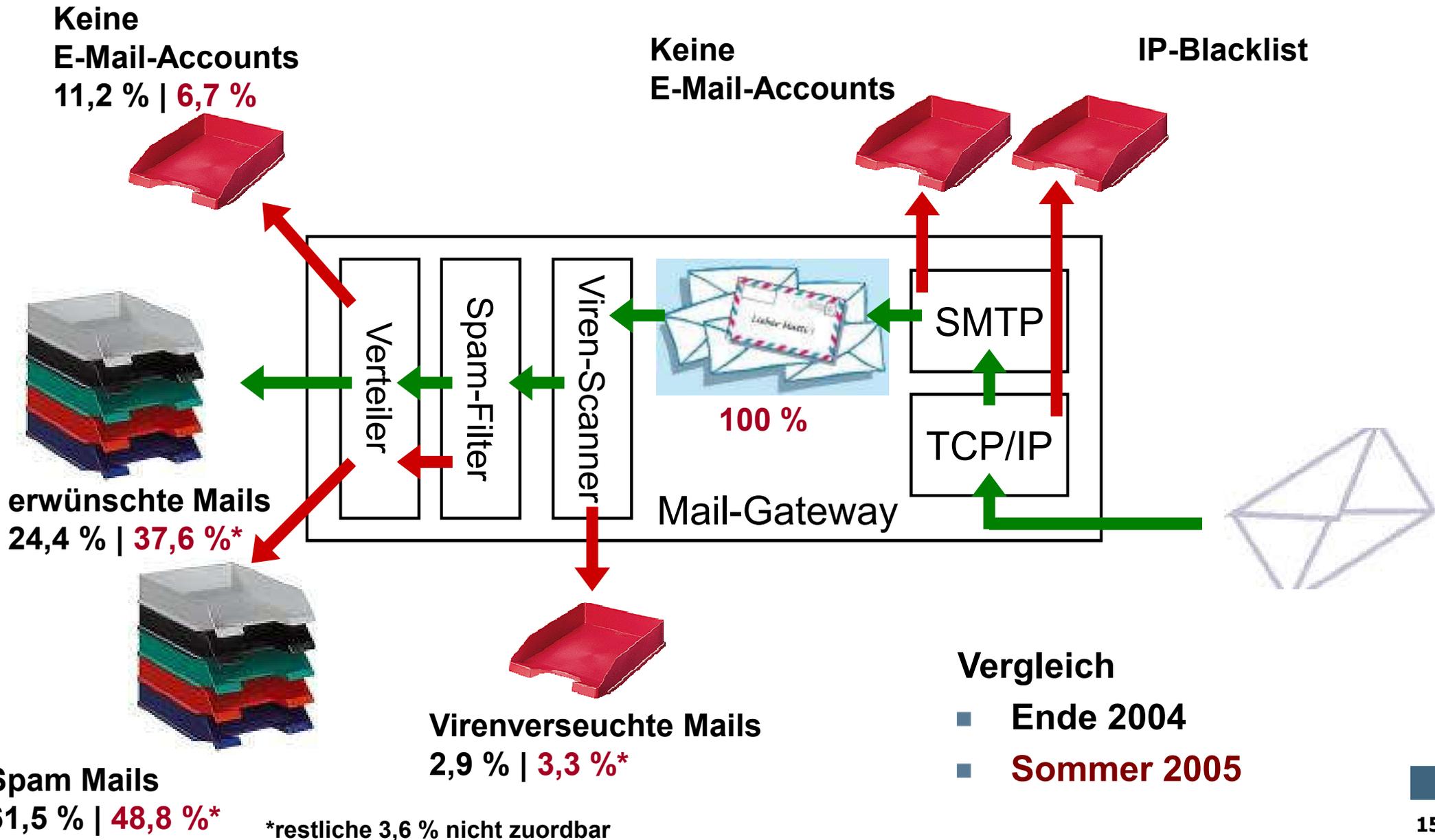
→ Ergebnisse: System, Eingang



- Vergleich**
- Ende 2004
 - Sommer 2005

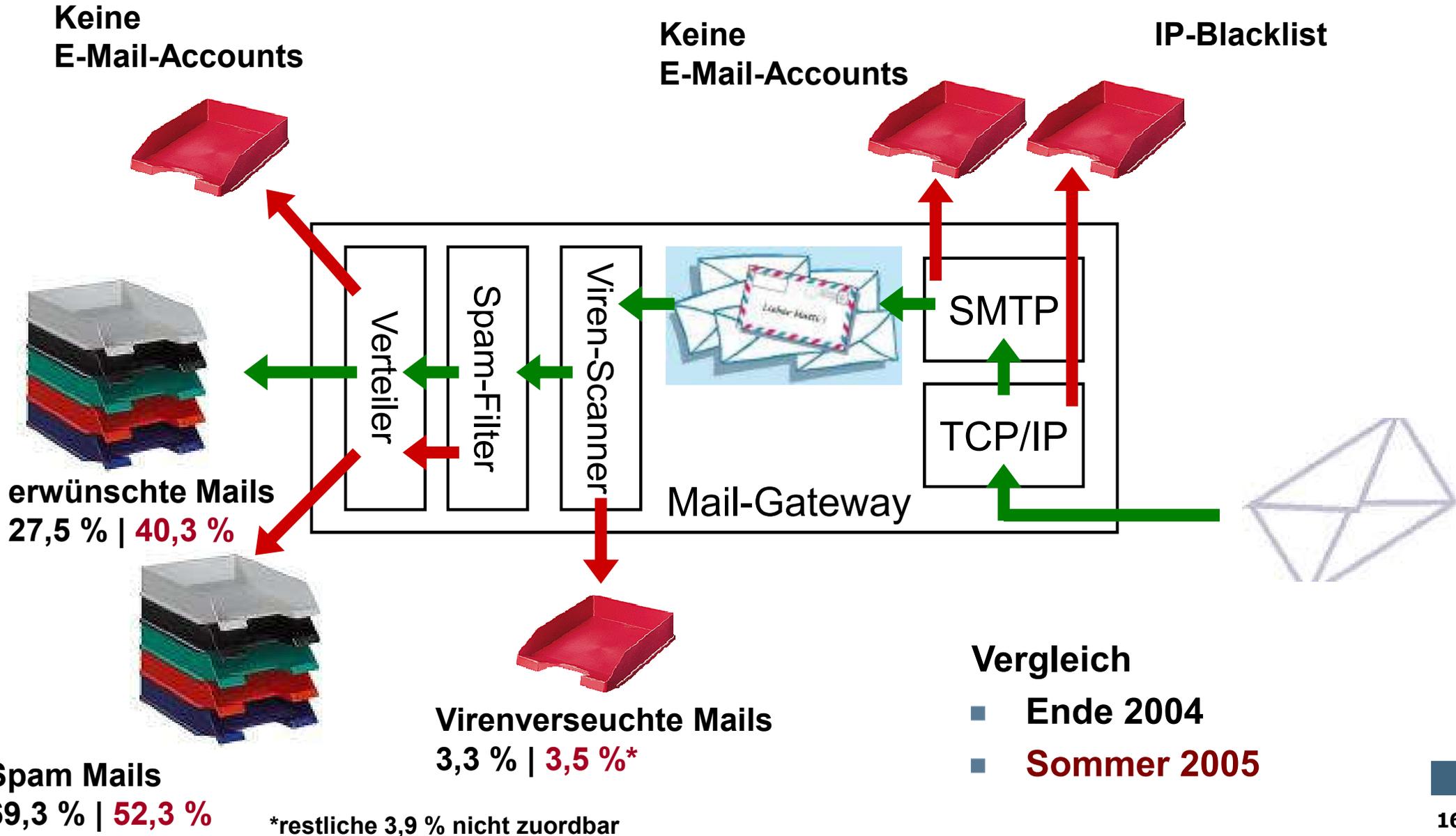
Generalisierte Sichtweise – Vergleich

→ Ergebnisse: System, angenommene



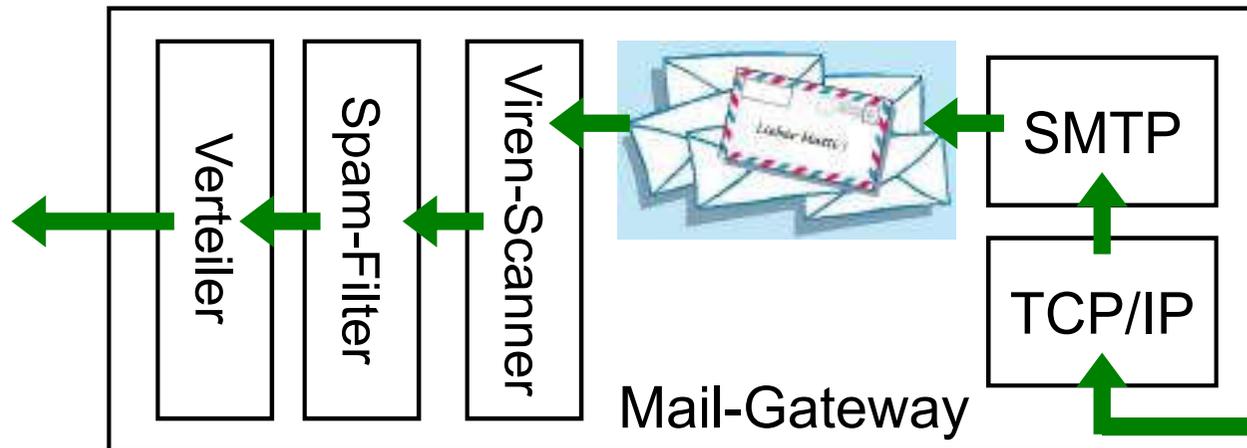
Generalisierte Sichtweise – Vergleich

→ Ergebnisse: Nutzerperspektive



E-Mail Verlässlichkeit

→ Verschlüsselte E-Mails



Rechtsform	
AG	2,1
Behörde	1,1
GmbH	5,3
Hochschule	0,3
ISP	0,5
andere	7,7
Gesamtergebnis	4,3

■ Verfahren:

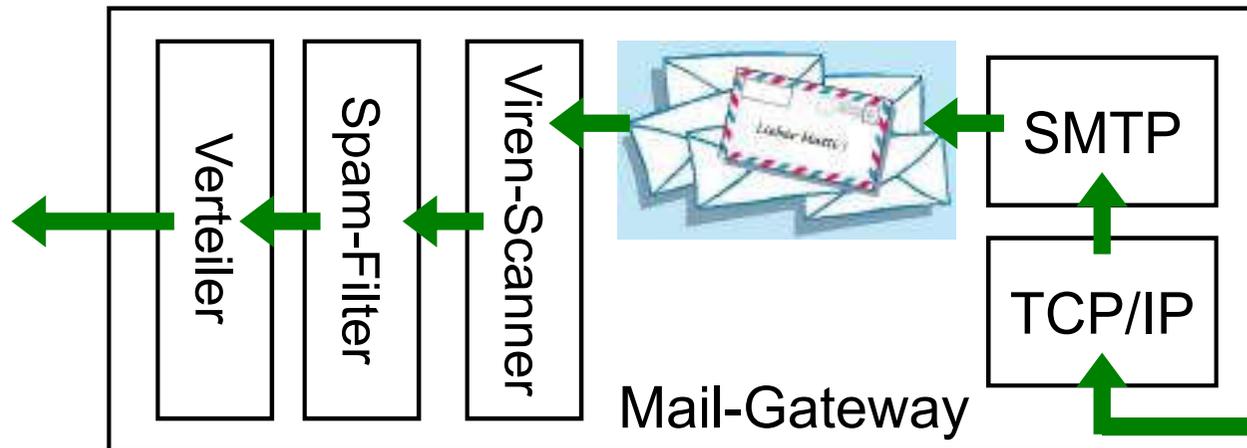
- PGP/OpenPGP/GPG: 36,7%
- S/MIME: 22,8%
- Passphrase-gestützt: 3,8%

E-Mail Verlässlichkeit

→ Signierte E-Mails

Password Fishing!

Branche	
Bildungsinstitution	0,0
Finanzdienstleistungen	21,2
Informationstechnologie	7,9
Öffentlicher Dienst	0,8
Industrie	0,3
Dienstleistungen	0,5
ISP	1,5
Gesamtergebnis	5,9



- **Widerspruch**
 - Über 45% der Befragten betreiben kritische Geschäftsprozesse auf E-Mail-Basis!

E-Mail Verlässlichkeit

→ Einschätzung der Bedrohungslage

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

Sehr gering	_____	Sehr hoch
<input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/>

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

Sehr gering	_____	Sehr hoch
<input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/>

Wie würden Sie die heutige Bedrohungslage (Spam) einschätzen?

Sehr gering	_____	Sehr hoch
<input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/>

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

Sehr gering	_____	Sehr hoch
<input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/>

- E-Mail Anwendung
- Umfrage „E-Mail Verlässlichkeit“
- **Einschätzung
„Viren, Würmer, Trojaner, ...“**
- Einschätzung „Spam“
- Digitale Signatur und Verschlüsselung
(Passwort Fishing)
- Zusammenfassung

Viren, Würmer, Trojaner, ...

→ Einschätzung

- Viren haben sich zu einem „**etablierten Problem**“ entwickelt.
- Weitere Herausforderungen
 - **Konsequente Umsetzung** von zentralen und dezentralen Anti-Viren Sicherheitsmechanismen
 - **Geschwindigkeit neuer Signaturen (Verwundbarkeitsfenster)**
 - In den letzten Jahren von 12 auf 10 Stunden reduziert
 - Ziel: 3 Stunden
 - vorausschauende Erkennungstechnologien
 - **Trusted Computing** in der Zukunft

- E-Mail Anwendung
- Umfrage „E-Mail Verlässlichkeit“
- Einschätzung „Viren, Würmer, Trojaner, ...“
- **Einschätzung „Spam“**
- Digitale Signatur und Verschlüsselung
(Passwort Fishing)
- Zusammenfassung

Spam

→ Einschätzung

- **Spam-Mails müssen reduziert werden!**
 - False Positive
 - Hoher Schaden
- **Die wichtigsten Antispam-Mechanismen sind:**
 - Spam-Filter für einen besseren Umgang mit unerwünschten E-Mails (keine Verhinderung)
 - Blocking-Verfahren (IP-ADR, E-Mail-ADR) zur Verhinderung eines Schadens (Bandbreite, Speicherplatz, Zeit des Benutzers, usw.)
 - Ordnung und deren Umsetzung zur Verhinderung eines Schadens (dynamische IP-Adressen austauschen und blocken, E-Mail nur über Smart-Host – sonst blocken von Port 25)
 - Digitale Signatur zur Vermeidung von Spam-Mails
 - Strafverfolgung zur Abschreckung von Spammern

- E-Mail Anwendung
- Umfrage „E-Mail Verlässlichkeit“
- Einschätzung „Viren, Würmer, Trojaner, ...“
- Einschätzung „Spam“
- **Digitale Signatur und Verschlüsselung**
- Zusammenfassung

E-Mail Sicherheit

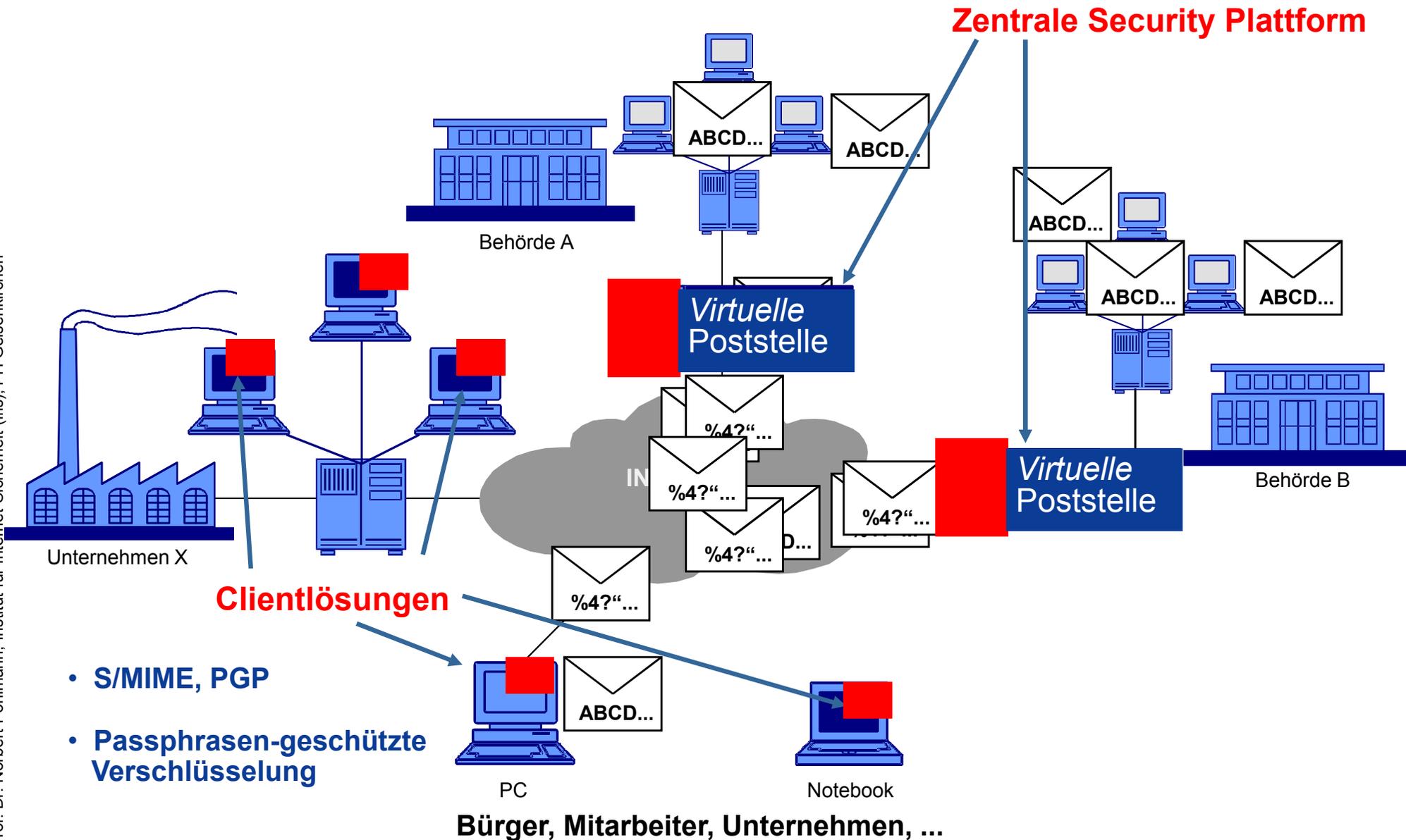
→ Sicherheitsdienste

- **Vertraulichkeit** der übertragenen (und gespeicherten) Informationen
- **Datenintegrität** der übertragenen (und gespeicherten) Informationen
- **Authentikation** für die angebotenen Anwendungen und der Person (z.B. E-Mail über Web)
- **Verbindlichkeit** der ausgetauschten Informationen und Prozesse
- **Protokollierung und Beweissicherung** der Aktionen, die über E-Mail durchgeführt wurden!

E-Mail Sicherheit in der Praxis

→ Virtuelle Poststelle und E-Mail Client Security

© Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit (ifis), FH Gelsenkirchen



- S/MIME, PGP
- Passphrasen-geschützte Verschlüsselung

- **Virtuelle Poststelle**
 - **Grundsätzliche Sicherheit** aller E-Mails



- **Client-Security in der eigenen Organisation**
 - **Höhere End-to-End-Vertraulichkeit** (z.B. Beihilfe) und
 - persönliche Digitale Signatur (qualifizierte Signatur)
 - **Weniger als 5%** der Personen müssen eine qualifizierte Signatur durchführen / brauchen End-to-End Vertraulichkeit
 - Sachbearbeiter für Fachanwendungen, z.B. Steuer
 - Vorstand/Geschäftsführer/Prokuristen/Einkäufer
 - ...



- E-Mail Anwendung
- Umfrage „E-Mail Verlässlichkeit“
- Einschätzung „Viren, Würmer, Trojaner, ...“
- Einschätzung „Spam“
- Digitale Signatur und Verschlüsselung
(Passwort Fishing)
- **Zusammenfassung**

E-Mail Verlässlichkeit

→ Zusammenfassung

- E-Mail ist eine sehr wichtige Anwendung, auf die wir nicht verzichten können!
- Das Risiko eines Schadens bei der E-Mail-Anwendung ist sehr hoch!
- Wir brauchen eine Kultur, wie wir mit E-Mail umgehen sollen (Passwort Fishing, Disziplin, usw...).
- **Wir sind selbst für die IT-Sicherheit verantwortlich!**
- Wir brauchen einen Viren- und Spam-Schutz, für die kontrollierte Annahme von E-Mails.
- Wie brauchen E-Mail-Verschlüsselung für die angemessene Vertraulichkeit.
- Wir brauchen die digitale Signatur und eine Archivierung für eine notwendige Verbindlichkeit der Prozesse.

Kein Platz für Spams und Viren – Lösungsbeispiele zum wirksamen Schutz vor der Gefahr der Online-Kommunikation

Vielen Dank für Ihre Aufmerksamkeit
Fragen ?

Prof. Dr. Norbert Pohlmann

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