Fachhochschule Gelsenkirchen

Sicherheitsrisiken bei E-Mail-Anwendungen

Prof. Dr. Norbert Pohlmann

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

if(is) institut für internet-sicherheit.

Inhalt

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

Inhalt

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

E-Mail-Anwendung
→ Idee

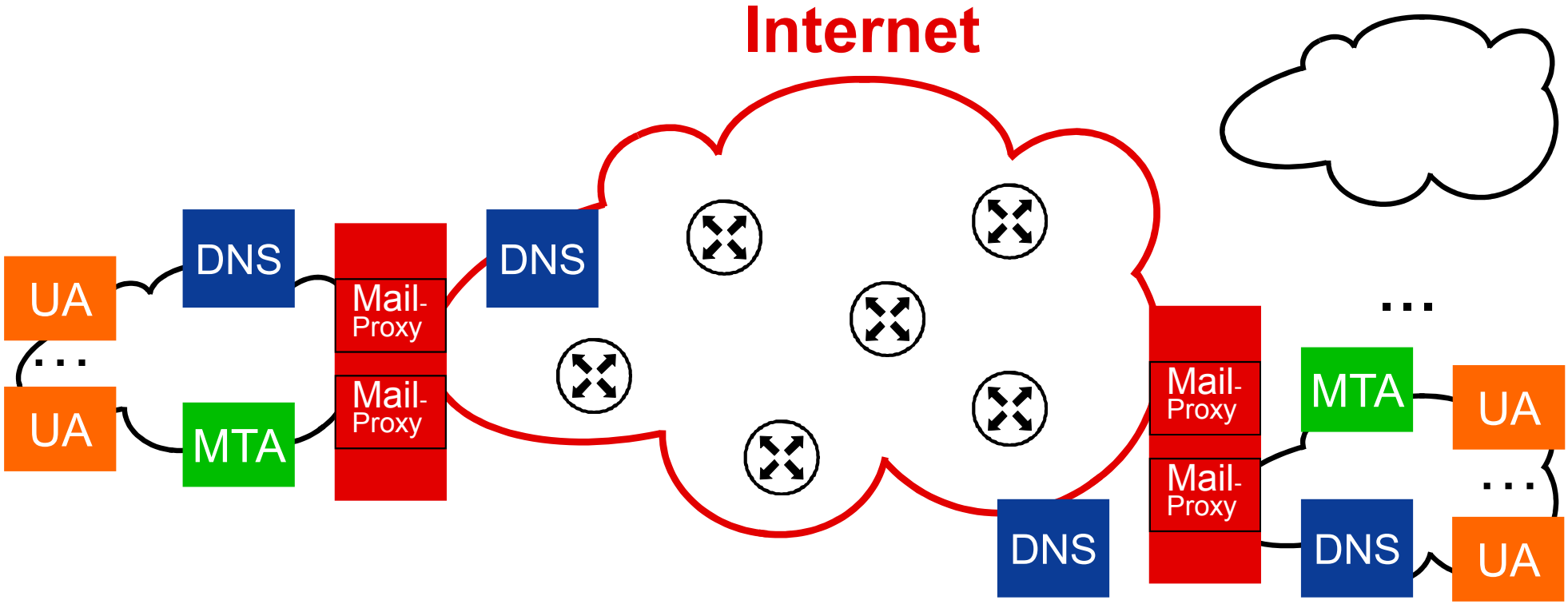
- E-Mail ist ein **textbasiertes Kommunikationswerkzeug**, mit dem weltweit einfach und schnell Informationen ausgetauscht werden können.

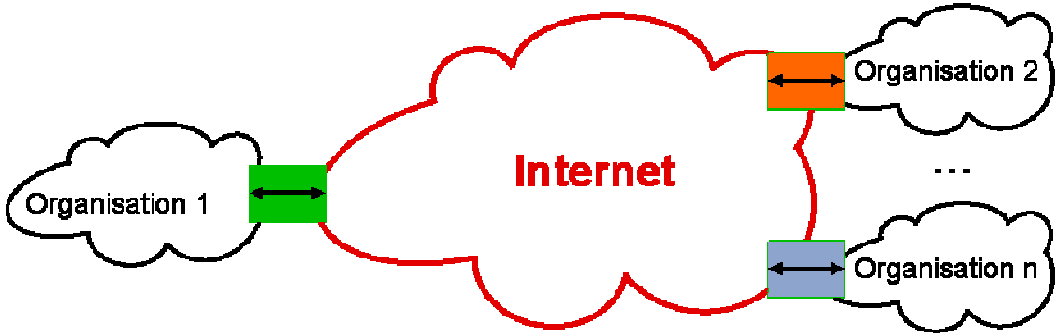
- E-Mail ist ein Ersatz für:
  - Die „Schneckenpost“: Postkarten, Briefe und Päckchen
  - Für Faxe

- 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 weiterverwendet werden
  - **Kostengünstig** – keine extra Kosten für den Transfer

E-Mail im gobalem Internet
→ Beispiel eines Szenario (Unternehmen)





Notwendige Sicherheitsdienste: Gewährleistung der

- Vertraulichkeit
- Authentikation
- Integrität
- Verbindlichkeit
- Verfügbarkeit

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 Anwendung
→ Realität (1/2)

- E-Mail macht 12% der Bandbreite im Backbone international agierender IP-Carrier aus.
- Pro Monat ca. 900 Mrd. E-Mails weltweit (sehr grobe Schätzung).
- 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 Anwendung
→ Realität (2/2)

- **E-Mail** ist für die Informationsgesellschaft **ein nicht mehr wegzudenkender Service.**
- **SPAM, Viren und andere Schwachstellen sind ein ernsthaftes Problem mit hohem Schaden.**
  - **Die E-Mail-Anwendung stellt ein sehr hohes Sicherheitsrisiko dar!**
- **Dieser Trend lässt die Frage zu, ob E-Mail in der nahen Zukunft noch genauso einfach und effizient eingesetzt werden kann wie bisher.**
- **Die positive Nutzung von E-Mails und damit die Informationsgesellschaft sind bedroht!**

Inhalt

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

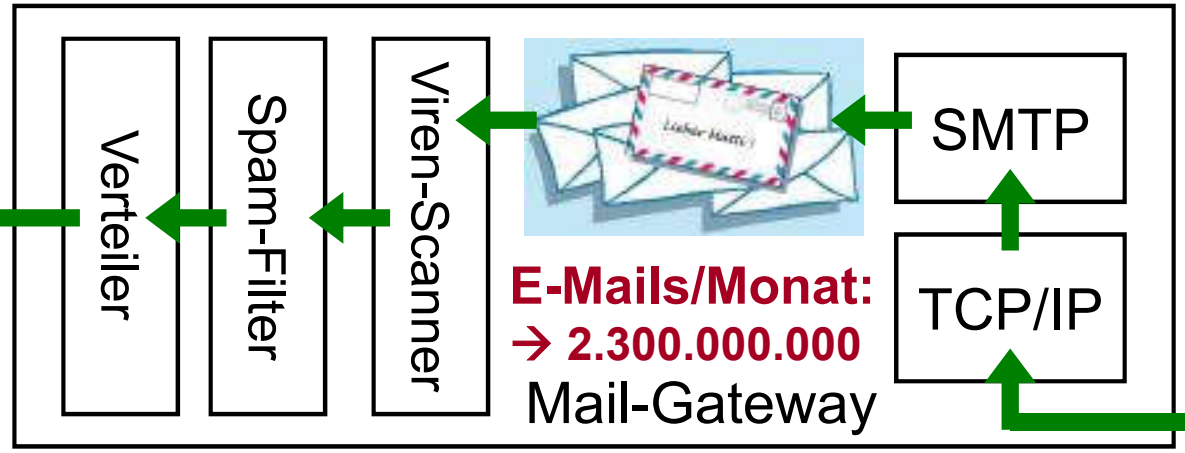
Ziele der Umfrage
→ E-Mail Verlässlichkeit

- Feststellung:
  - 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 Daten sich über die Zeit verändern

Allgemeine Statistik
→ Generalisierte Sichtweise

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

Teilnehmer:
→ 119



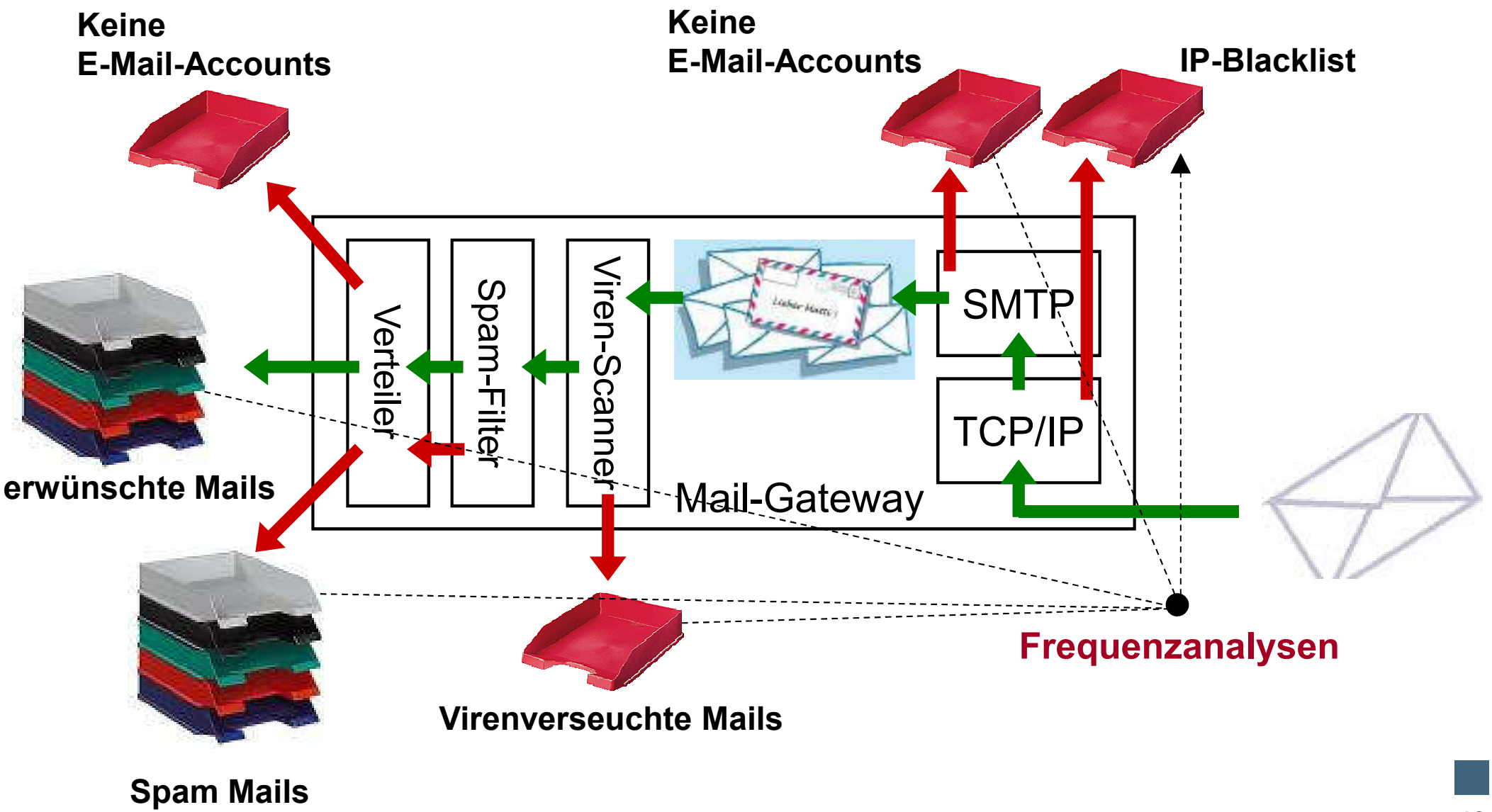
E-Mails/Monat:
→ 2.300.000.000

E-Mail-Accounts:
→ 40.000.000

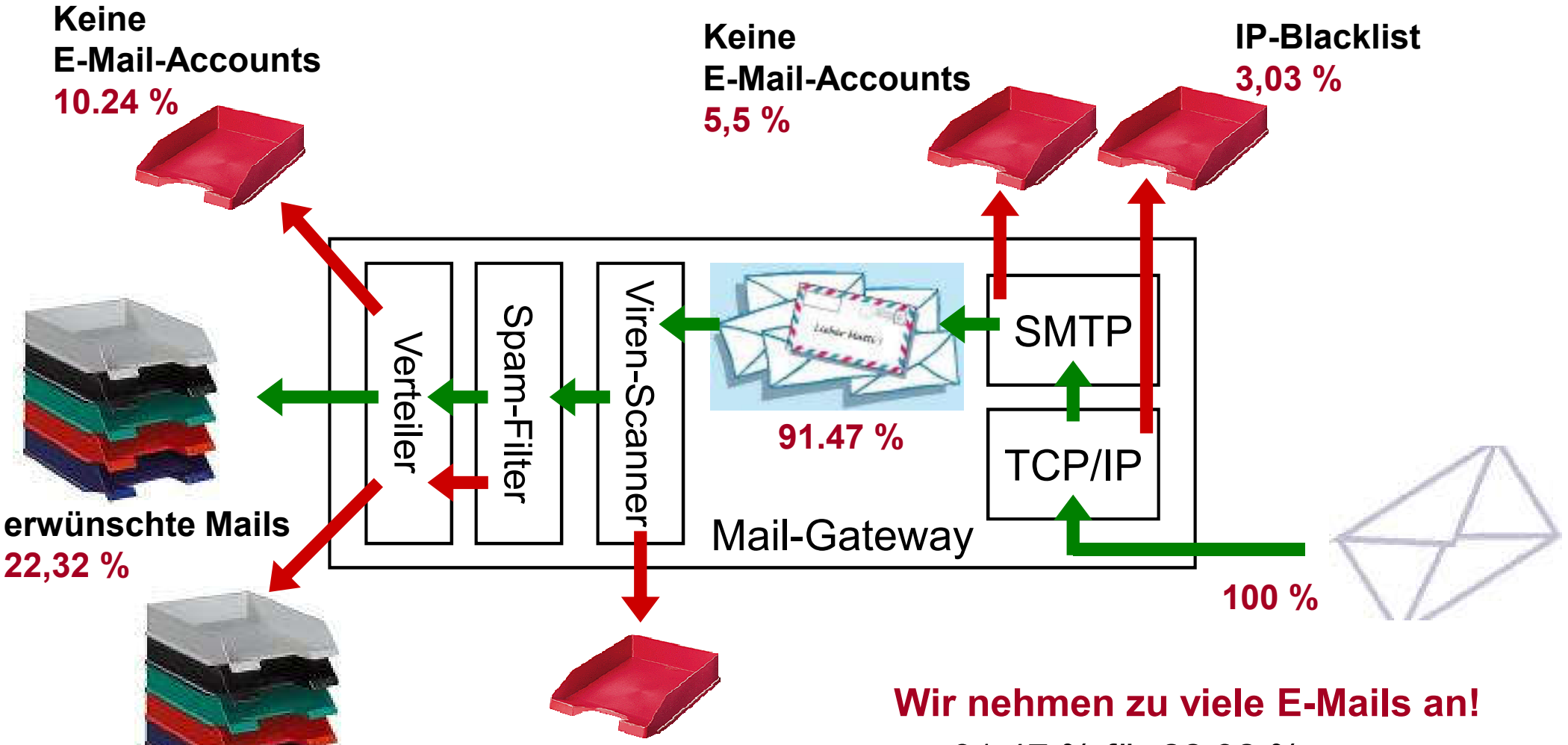
- Pro **AG**
  ca. 80 T E-Mail-Adressen
- Pro **GmbH**
  ca. 3 T E-Mail-Adressen
- Pro **ISP**
  ca. 5,5 Mio. E-Mail-Adressen

- 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



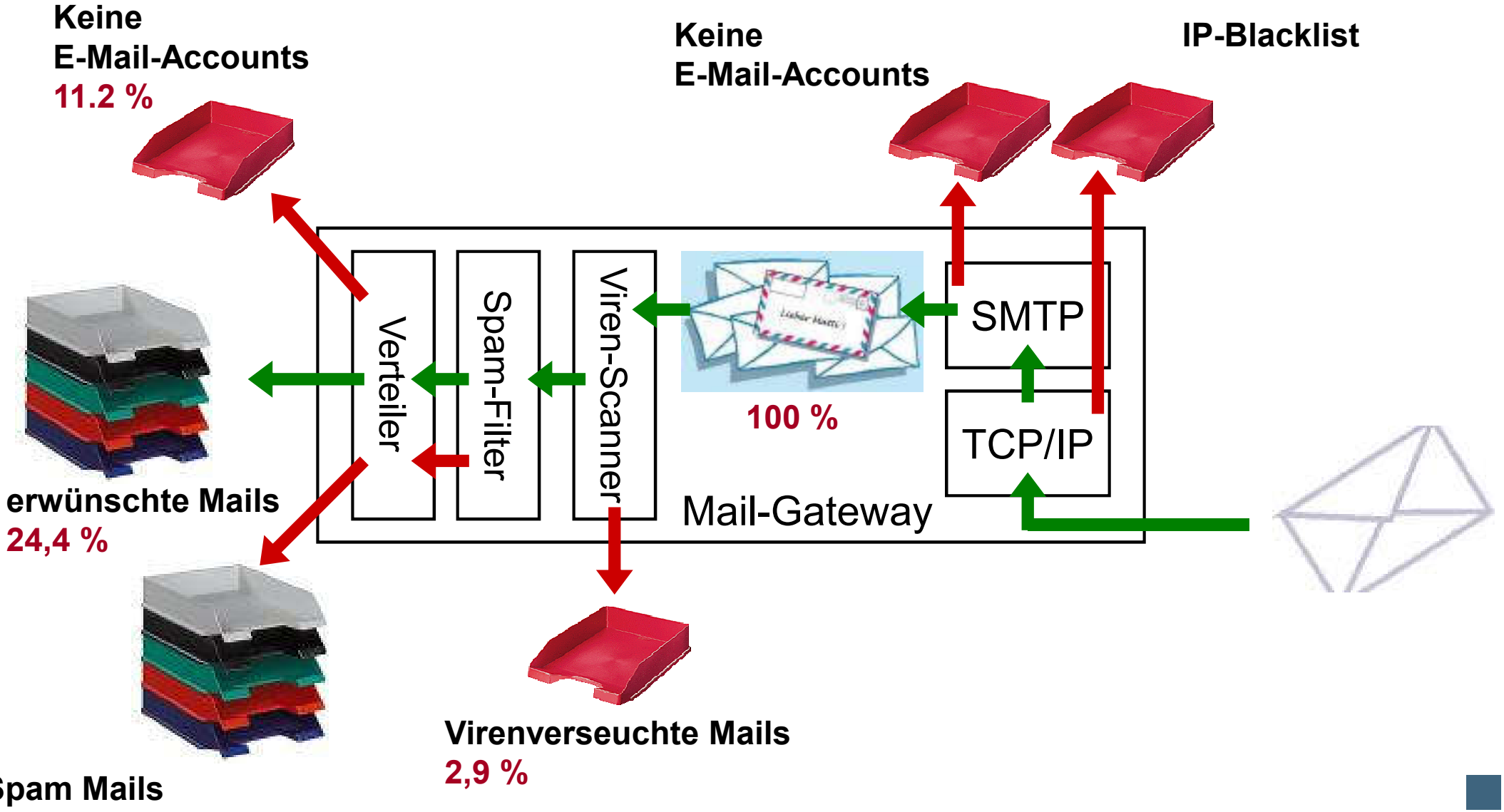
Generalisierte Sichtweise
→ Ergebnisse: System, Eingang



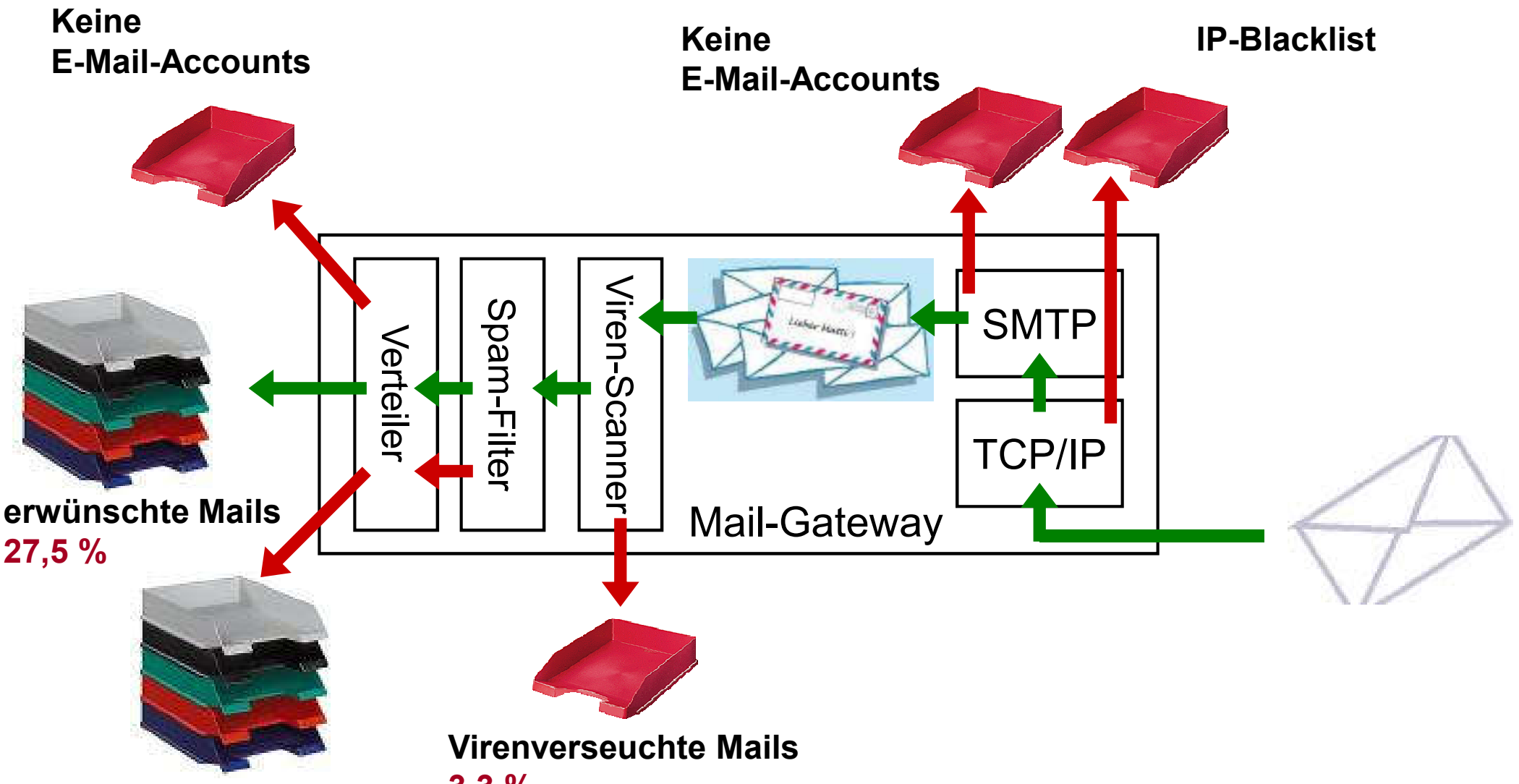
Wir nehmen zu viele E-Mails an!

- 91,47 % für 22.32 %
- Schaden: 1. Mrd. €
  (50 Cent/Mail)

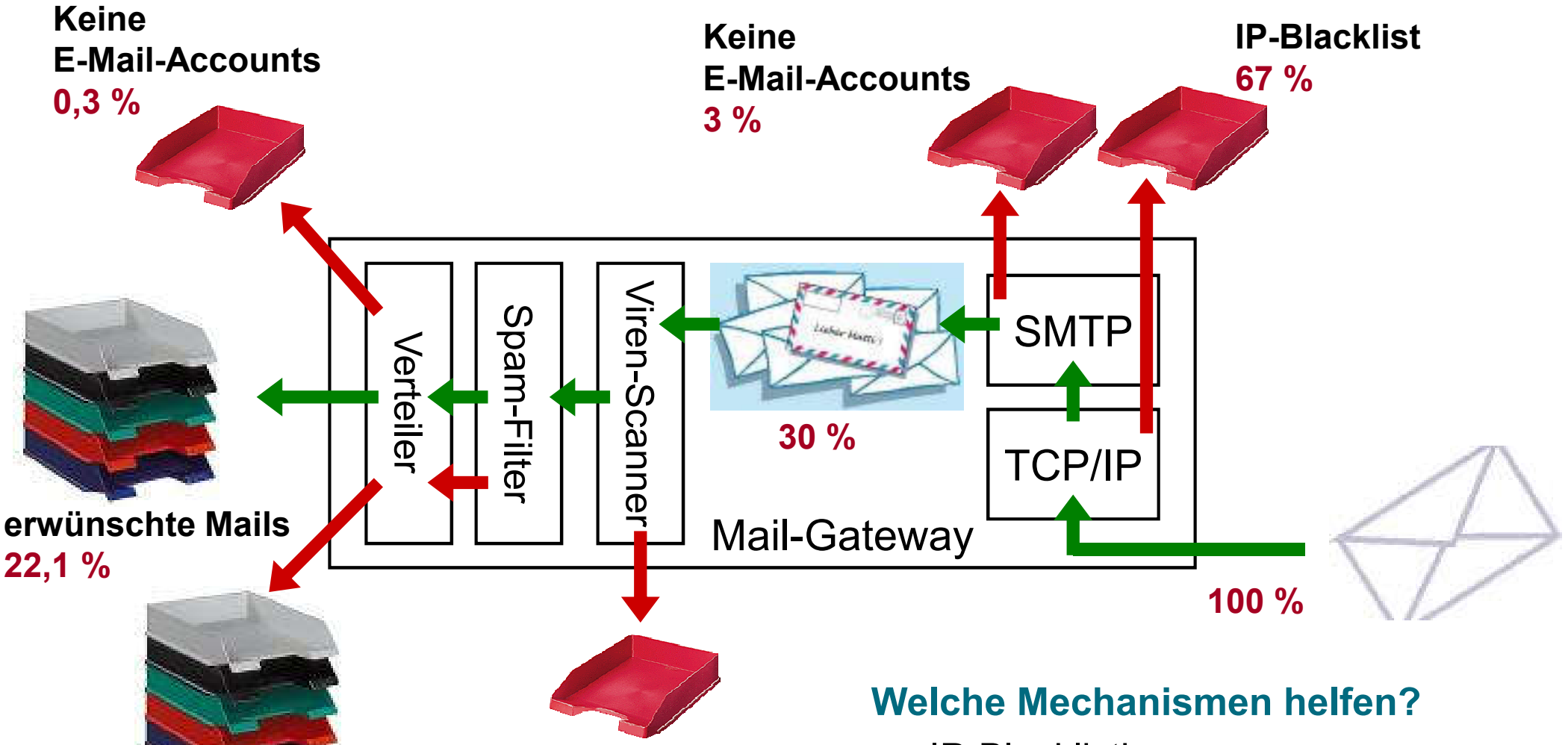
Generalisierte Sichtweise
→ Ergebnisse: System, angenommene



Generalisierte Sichtweise
→ Ergebnisse: Nutzerperspektive



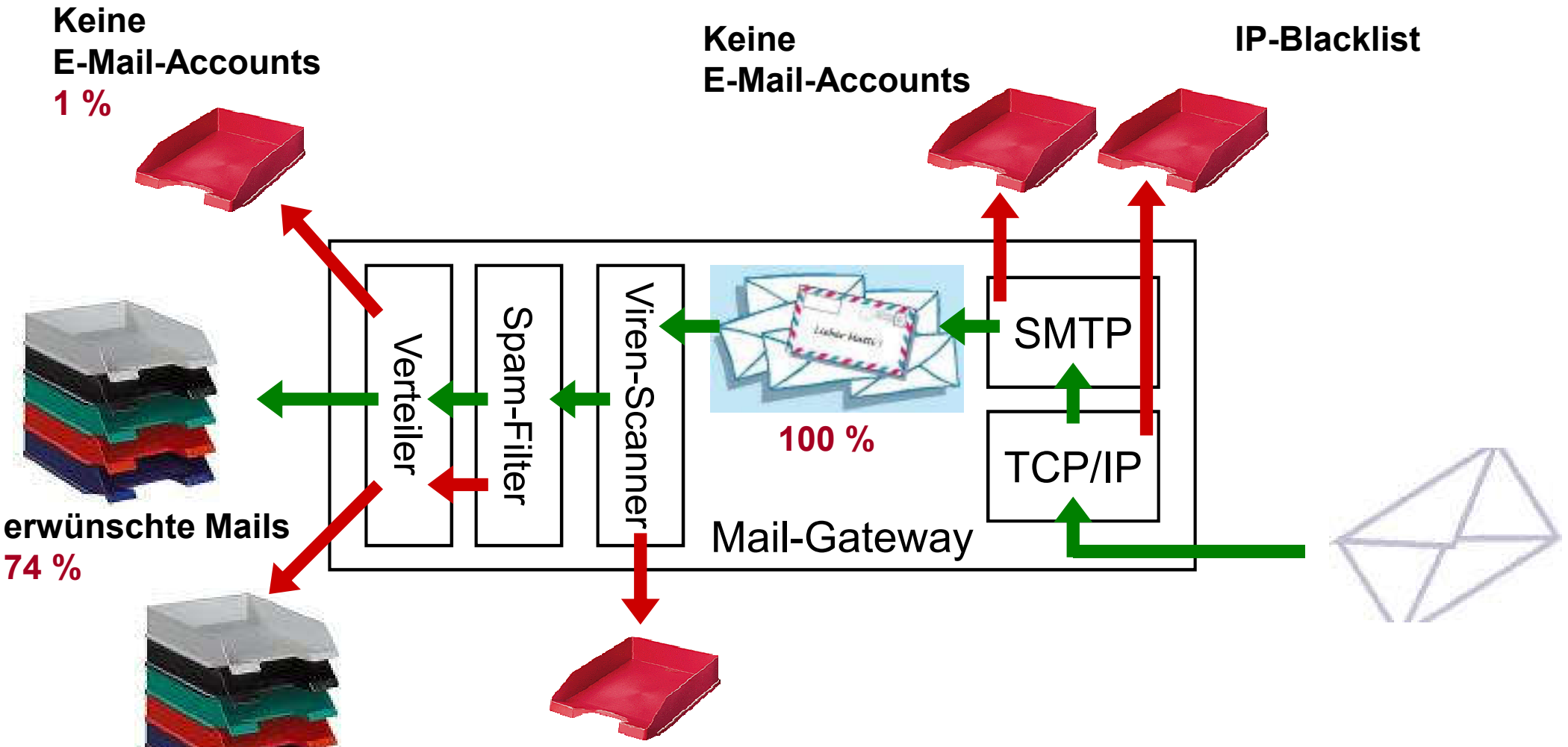
E-Mail Verlässlichkeit
→ Ideen/Empfehlungen: System, Eingang



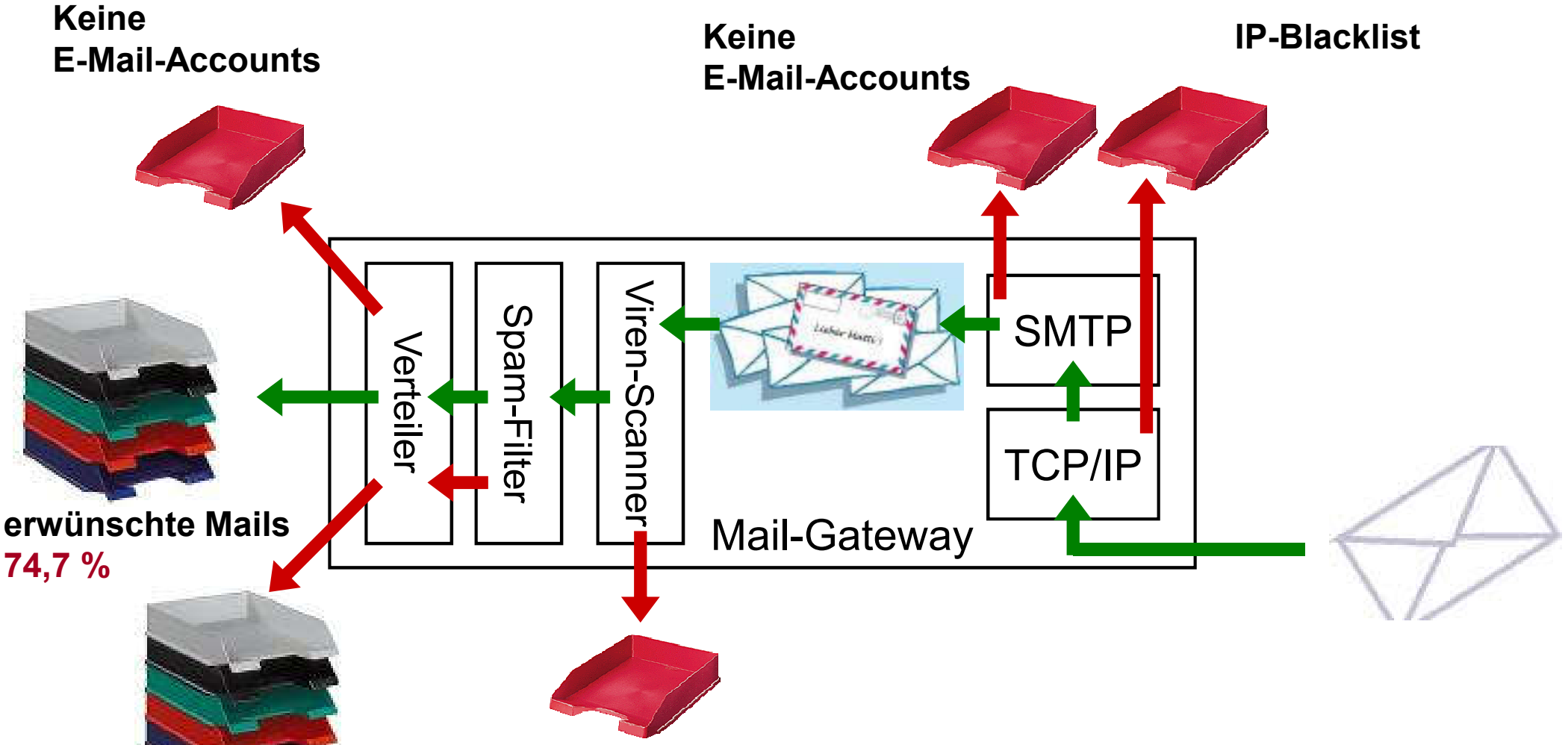
Welche Mechanismen helfen?

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

E-Mail Verlässlichkeit
→ Ideen/Empfehlungen: System, ange.

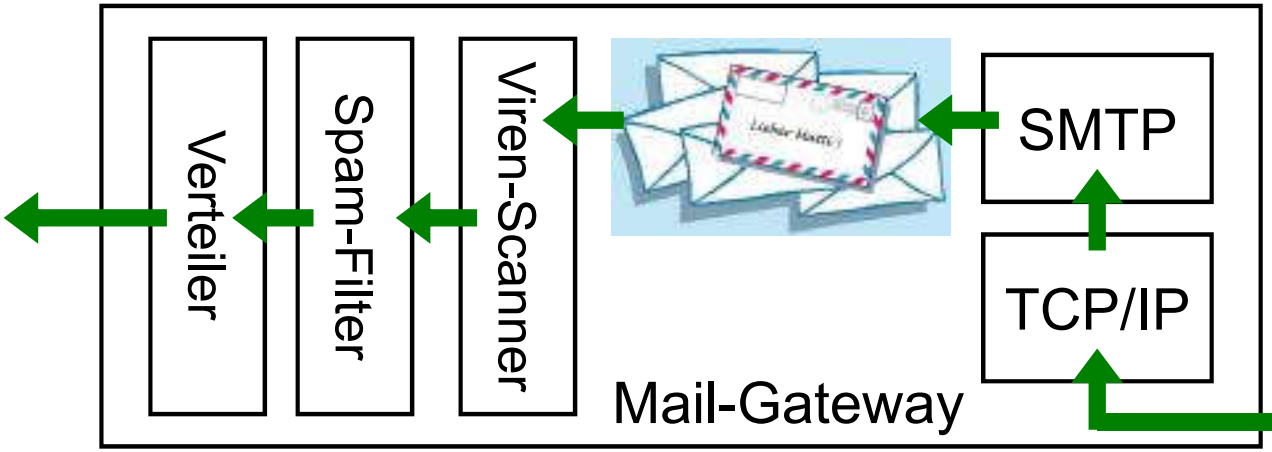


E-Mail Verlässlichkeit
→ Ideen/Empfehl.: Nutzerperspektive



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**

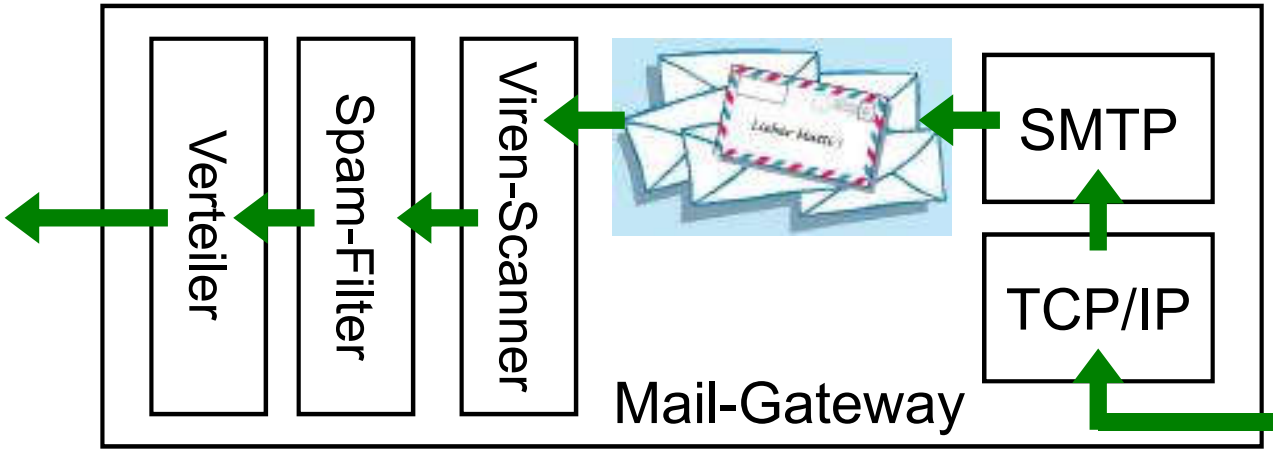


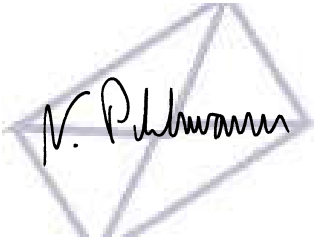
- **Verfahren:**
  - PGP/OpenPGP/GPG: 36,7%
  - S/MIME: 22,8%
  - Passphrase-gestützt: 3,8%

E-Mail Verlässlichkeit
→ Signierte E-Mails

Branche	
Bildungsinstitution	0,0
Finanzdienst-leistungen	21,2
Informations-technologie	7,9
Öffentlicher Dienst	0,8
Industrie	0,3
Dienstleistungen	0,5
ISP	1,5
Gesamtergebnis	**5,9**

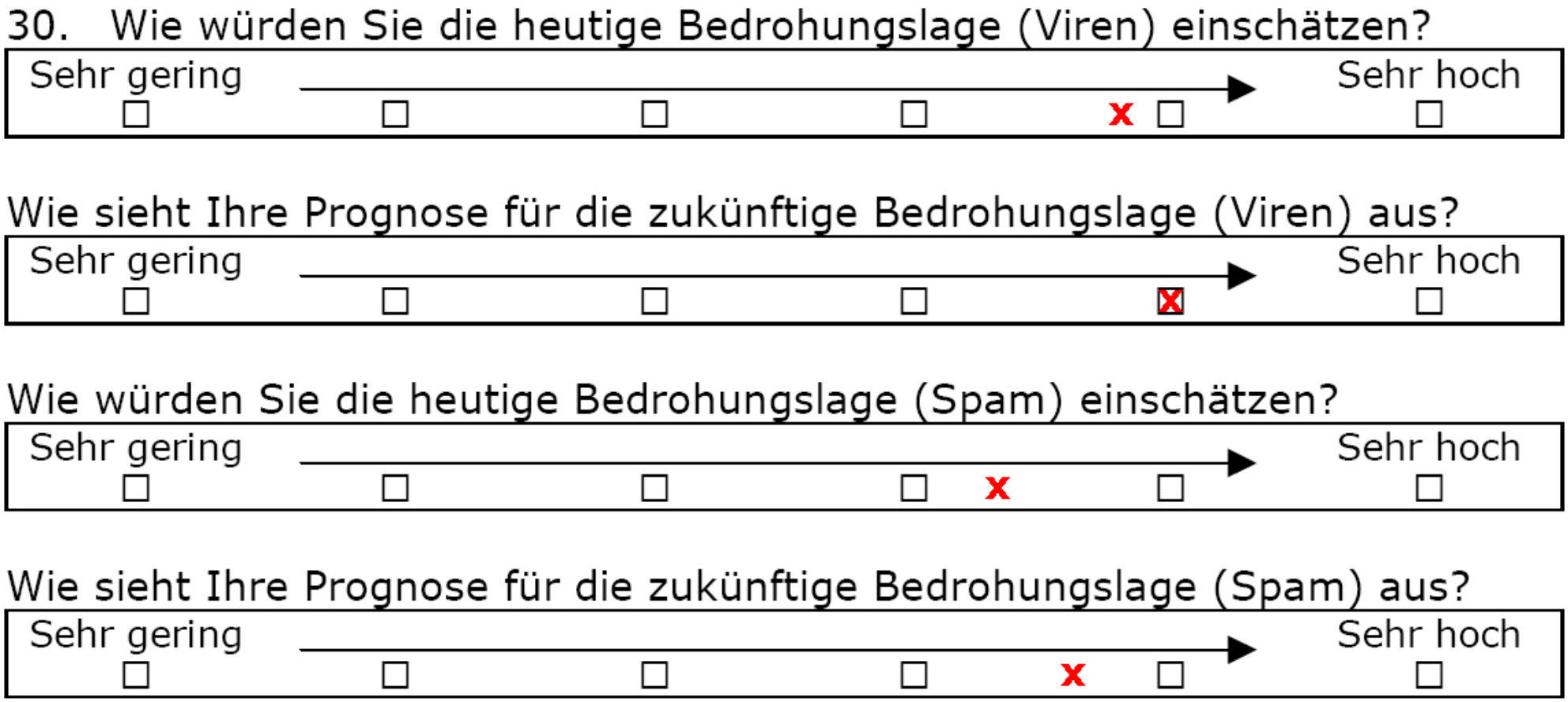
Passwort Fishing!





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

E-Mail Verlässlichkeit
→ Einschätzung der Bedrohungslage



Zeitraum des 2. Laufs: 06.06.2005 - 24.06.2005

Inhalt

- 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
    - vorausschauenden Erkennungstechnologien
  - **Trusted Computing** in der Zukunft

Inhalt

- 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-Mechansimen 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

Inhalt

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

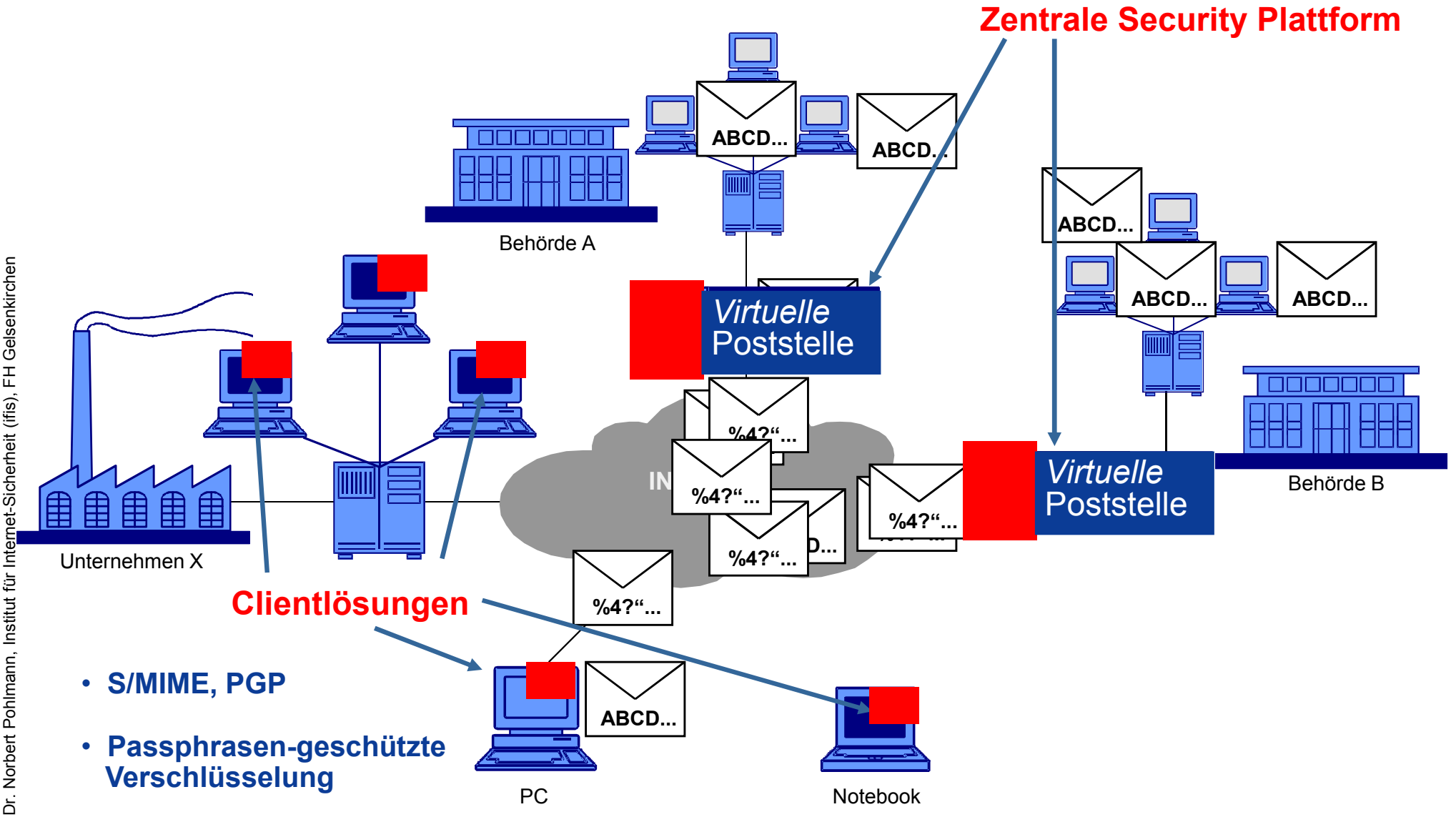
E-Mail Sicherheit
→ Sicherheitsdienste

institut für internet-sicherheit.

- **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 Clients



E-Mail Sicherheit
→ Warum eine *virtuelle* Poststelle?

- **Pragmatischer Ansatz, weil ...**
  - die notwendigen Standards bei unterschiedlichen Herstellern nicht zustandekommen oder zu lange dauern
  - auch die virtuelle Welt nicht ideal ist

- **Eine zentrale Security Plattform, weil ...**
  - sie passgenau ist (Sicherheit umsetzbar machen)
  - sie als modulare Plattform für hohe Flexibilität sorgt
  - sie zukunftssicher ist (das Sicherheitssystem wächst mit den Anforderungen)
  - sehr gutes Kosten-/Nutzenverhältnis hat

E-Mail Sicherheit
→ Probleme bei End-to-End-Lösungen

- **Keine verbreitete Installationsbasis**
  - Kaum Einsatz von PKI (Zertifikat-Management)
  - Clients: Empfänger können nicht entschlüsseln/verifizieren
- **Hohe Kosten für Infrastruktur**
  - Alle SW-Clients mit E-Mail Security Applikation
  - Token (z.B. SmartCards), SmartCard-Reader
  - Rollout ist sehr aufwendig
  - Updates
  - Helpdesk ist notwendig
  - Schulung aller Mitarbeiter, Nutzung und Verwendung
  - Zertifikatsmanagement (PKI)
- **Alleinige Kontrolle bei Benutzer**
  - Verantwortung, wann verschlüsselt und signiert werden soll
  - Recovery Probleme (Mitarb. krank, verliert SmartCard (SC), SC defekt, ...)
  - Keine Vertreterregelung

Anwendungsvergleich E-Mail Sicherheit

Anwendung	Zentral/Gateway	Client
Benutzerfreundlichkeit	+	-
Signatur und Verschlüsselung großer Mailvolumina	+	-
Elektronische Signatur	+	+
Qualifizierte Signatur	- (evtl. auch +)	+
Umsetzung der Organisationspolicy	+	o (Vertrauen auf Anwender)
Vertreterregelung	+	-
Recovery	+	o (Nur wenn Anwender mit Organisationskey mitverschlüsselt)
Mails mit hoher interner Vertraulichkeit	-	+
Virenscanning, Inhaltsprüfung	+	-

!Hybrid Lösung ist der Königsweg! (VP+Clients)

Gemischte Anwendung

- ***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
    - ...

Inhalt

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

E-Mail Verlässlichkeit
→ Zusammenfassung

institut für internet-sicherheit.

- **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.**
- **Wir sollten ein Infrastruktur zur Verfügung stellen, die eine digitale Signatur und die E-Mail-Verschlüsselung einfach ermöglicht.**
- **Identity-Management (PKI)**
  - Identifikation und Verifikation der Personen im Internet möglich machen (ID-Card)!

Weitere Maßnahmen
→ Ordnung schaffen

- „Die Kunst des Forschrittes besteht darin,
  - **Ordnung inmitten der Veränderung** zu bewahren und
  - **Veränderung inmitten der Ordnung**“
    → *Alfred North Whitehead - britischer Philosoph und Mathematiker*

- Wie brauchen mehr Ordnung im Internet, damit ein weiterer Fortschritt möglich ist!
  - **Wir müssen anfangen mehr Ordnung zu schaffen und umzusetzen, wie im Straßenverkehr, damit Spam und co. wirksam entgegengewirkt werden kann.**
  - **Organisierte Listen (White and Black)**
    - Bekannte E-Mailer, dynamische IP-Adressen, Spammer

Fachhochschule Gelsenkirchen

Sicherheitsrisiken bei E-Mail-Anwendungen

Vielen Dank für Ihre Aufmerksamkeit
Fragen ?

Prof. Dr. Norbert Pohlmann

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

if(is) institut für internet-sicherheit.