Fachhochschule Gelsenkirchen

Sicherheit im E-Mail-Verkehr (Spam)

Prof. Dr. Norbert Pohlmann

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

Inhalt

- **E-Mail Anwendung**
- **Umfrage „E-Mail Verlässlichkeit“**
- **Einschätzung „Viren, Würmer, Trojaner, …“**
- **Spam**
- **Zusammenfassung**

Inhalt

- **E-Mail Anwendung**
  - Umfrage „E-Mail Verlässlichkeit“
  - Einschätzung „Viren, Würmer, Trojaner, …“
  - Spam
  - 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 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 Anwendung
→ Realität

- 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 Anwendung
→ Wo liegen die Gefahren?

- **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 wir 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.)

Inhalt

- E-Mail Anwendung
- **Umfrage „E-Mail Verlässlichkeit“**
- Einschätzung „Viren, Würmer, Trojaner, …“
- Spam
- Zusammenfassung

Ziele der Umfrage
→ E-Mail Verlässlichkeit

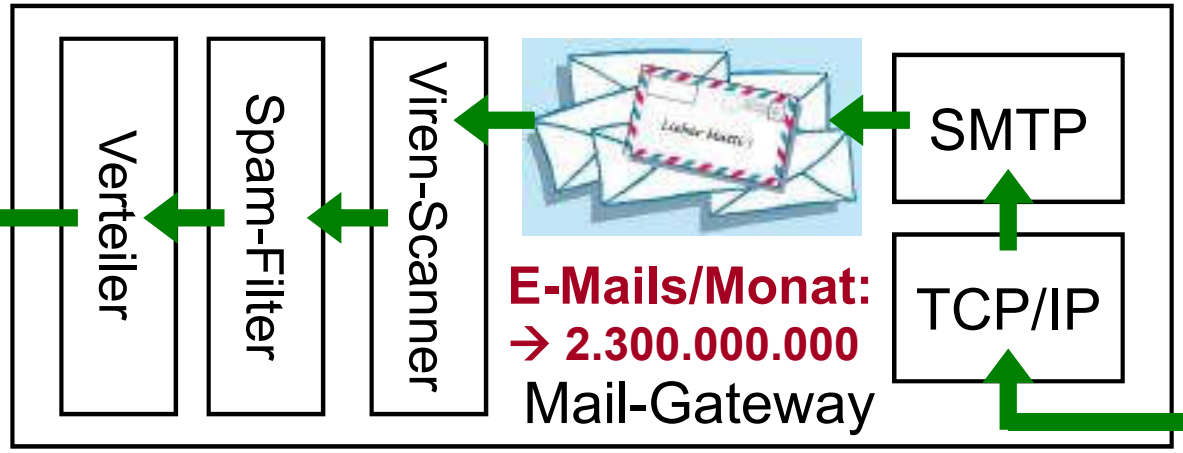
- Feststellung bezüglich:
  - Der Art der Informationen, die per E-Mail ausgetauscht werden
  - Der Anteilsverteilung des E-Mail-Volumens (Spam, Viren und Co.)
  - Des aktuellen Bedrohungszustandes
  - Der eingesetzten Gegenmaßnahmen
  - Welche Aspekte sich über die Zeit verändern

Vollständige Auswertungen siehe: www.internet-sicherheit.de

Allgemeine Statistik
→ Generalisierte Sichtweise

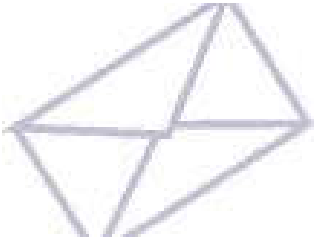
Rechtsform	
AG	13
Behörde	34
GmbH	28
Hochschule	9
ISP	7
Andere	28
Gesamt	**119**

Teilnehmer:
→ 119



E-Mails/Monat:
→ 2.300.000.000

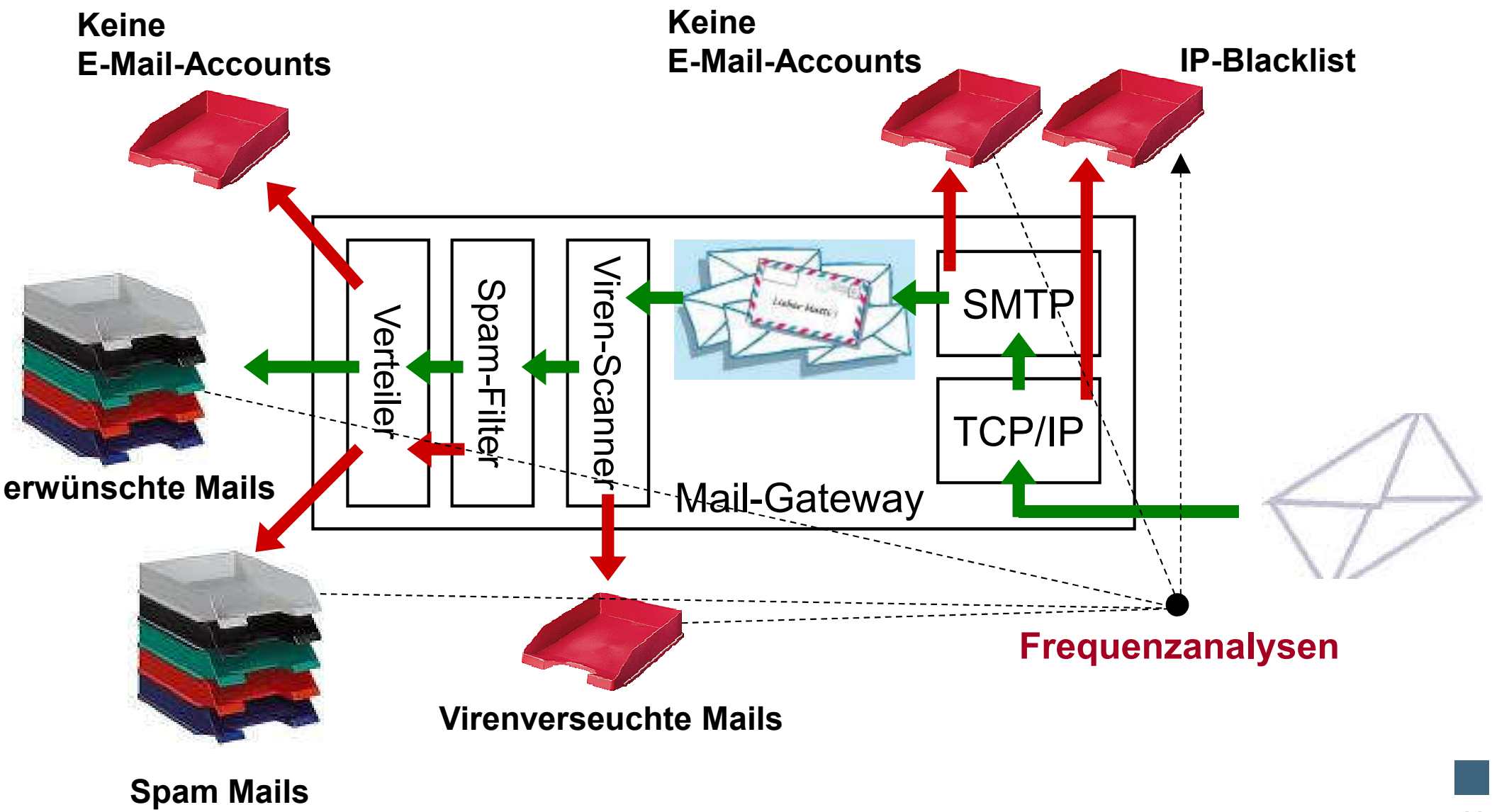
E-Mail-Accounts:
→ 40.000.000



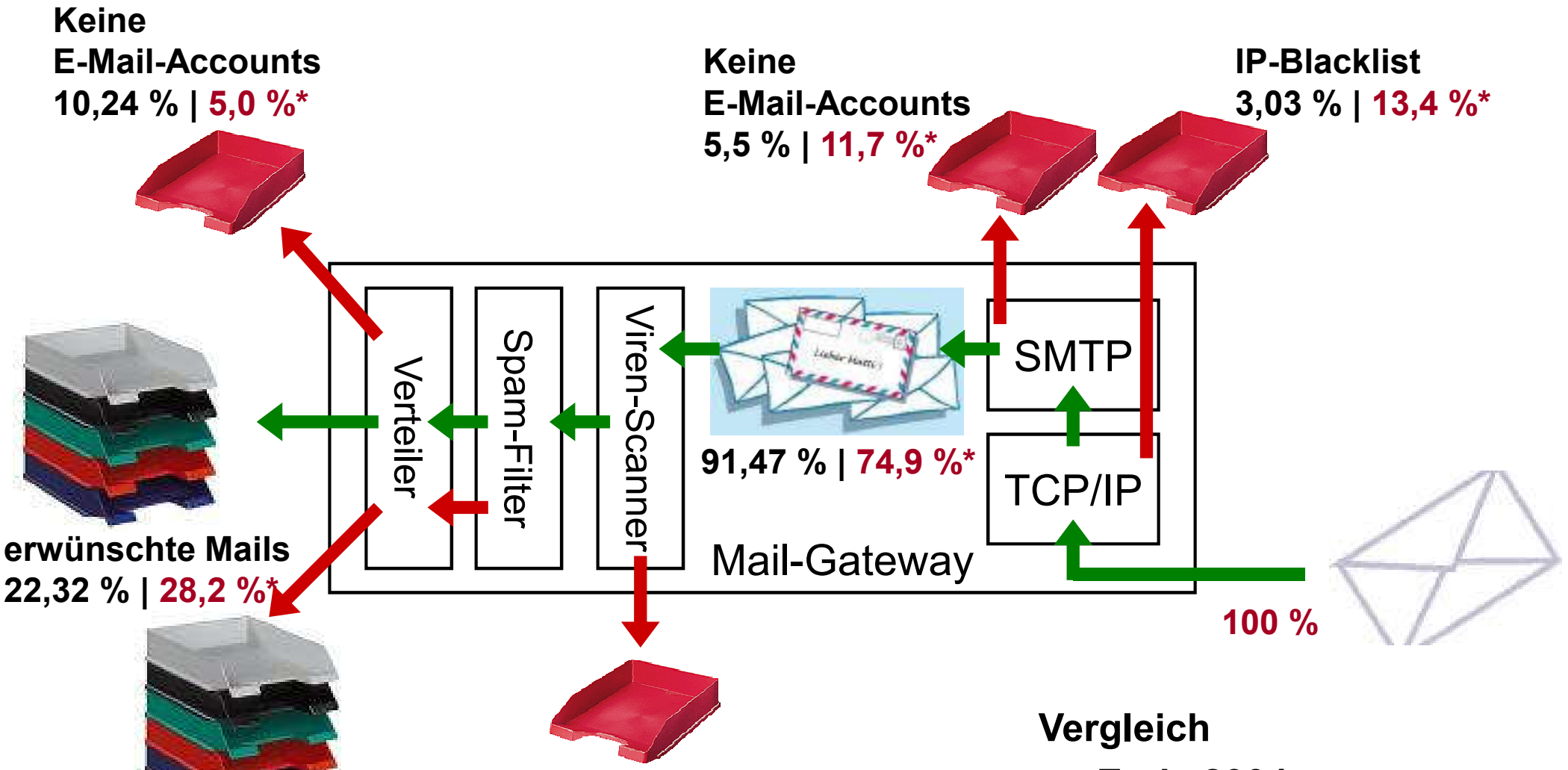
- Pro **AG**
  ca. 80 T E-Mail-Adressen
- Pro **GmbH**
  ca. 3 T E-Mail-Adressen
- Pro **ISP**
  ca. 5,5 Mio. E-Mail-Adressen

- 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 – Vergleich → Ergebnisse: System, Eingang

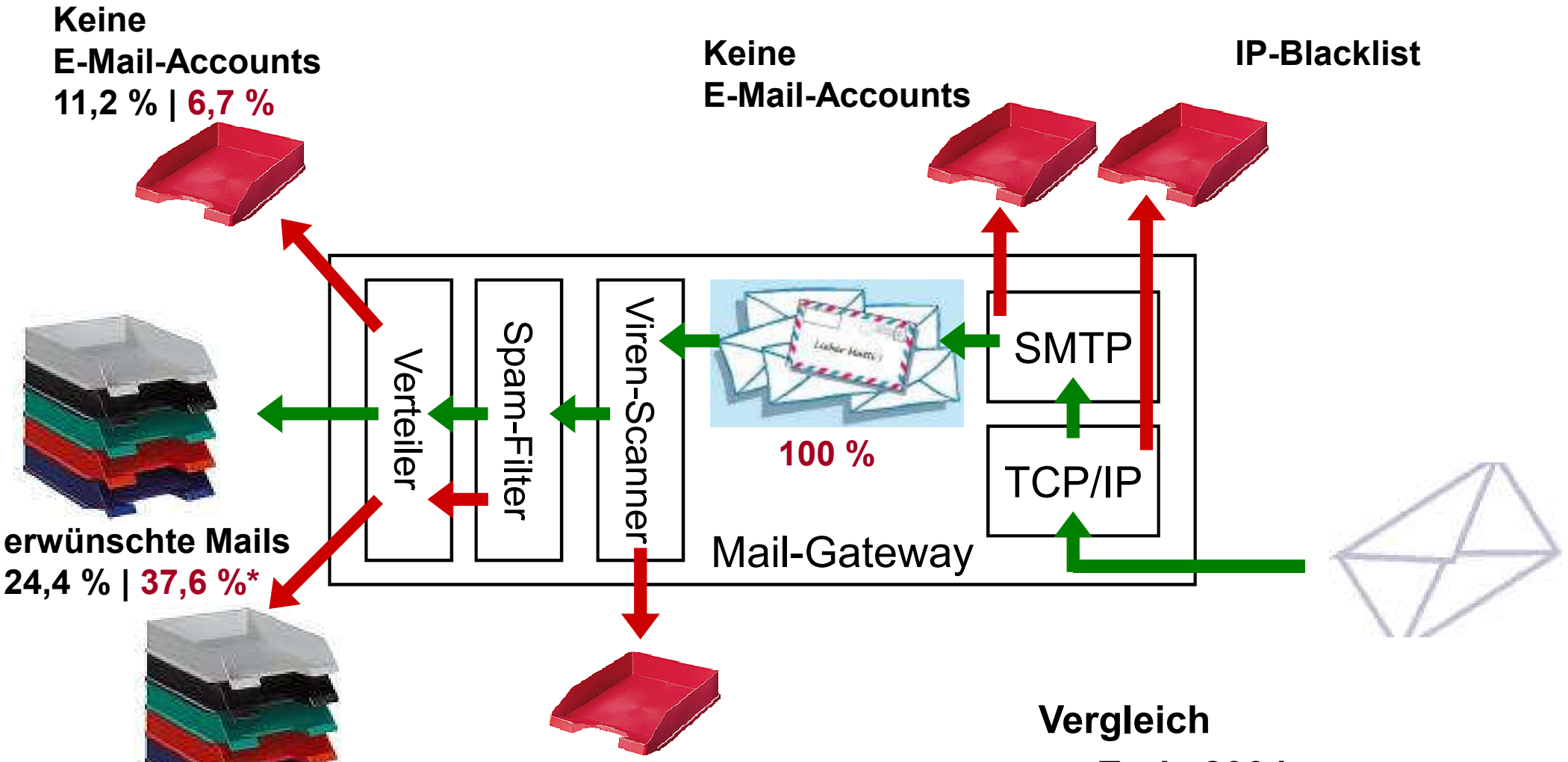


Vergleich

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

*restliche 2,7 % nicht zuordbar

Generalisierte Sichtweise – Vergleich → Ergebnisse: System, angenommene

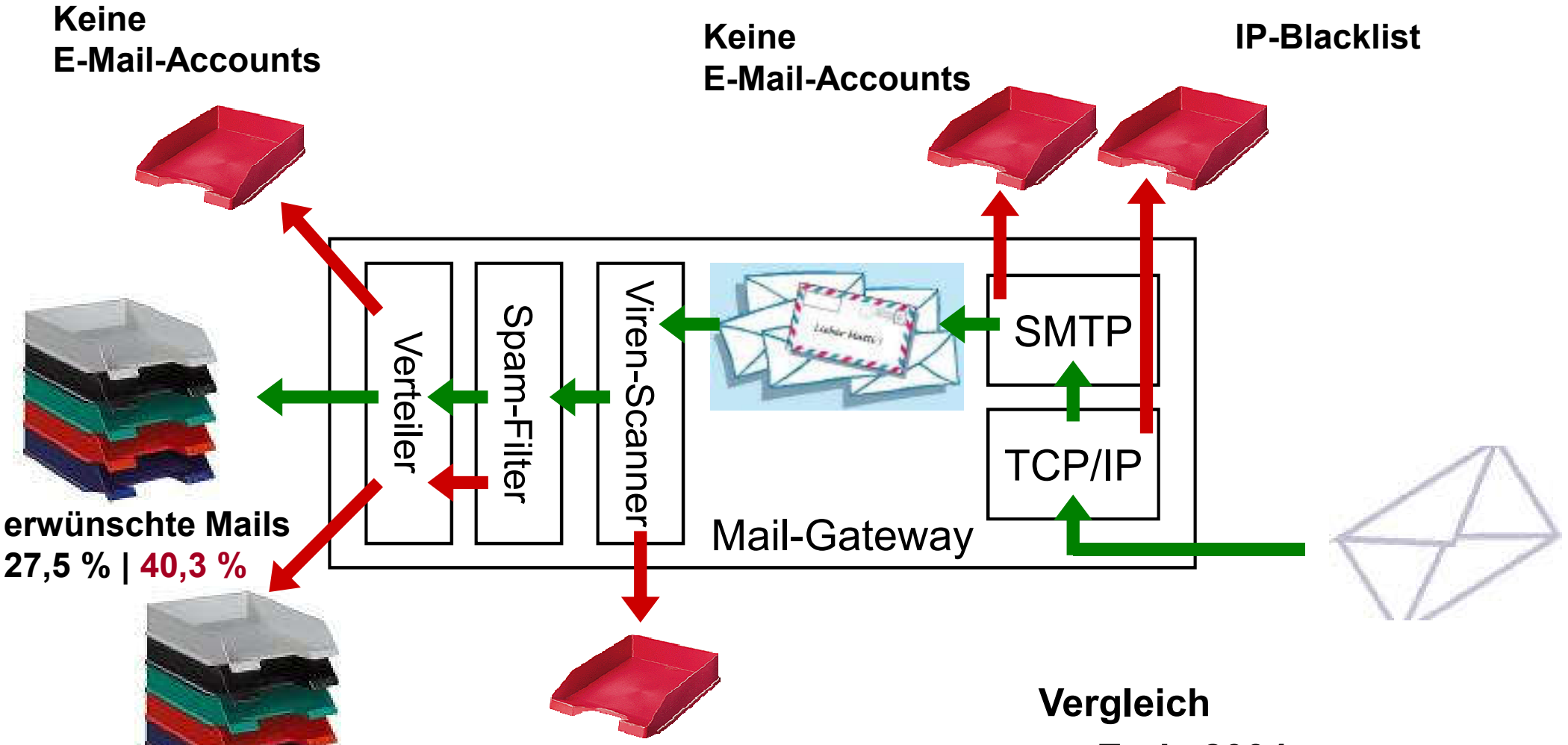


Vergleich

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

*restliche 3,6 % nicht zuordbar

Generalisierte Sichtweise – Vergleich
→ Ergebnisse: Nutzerperspektive



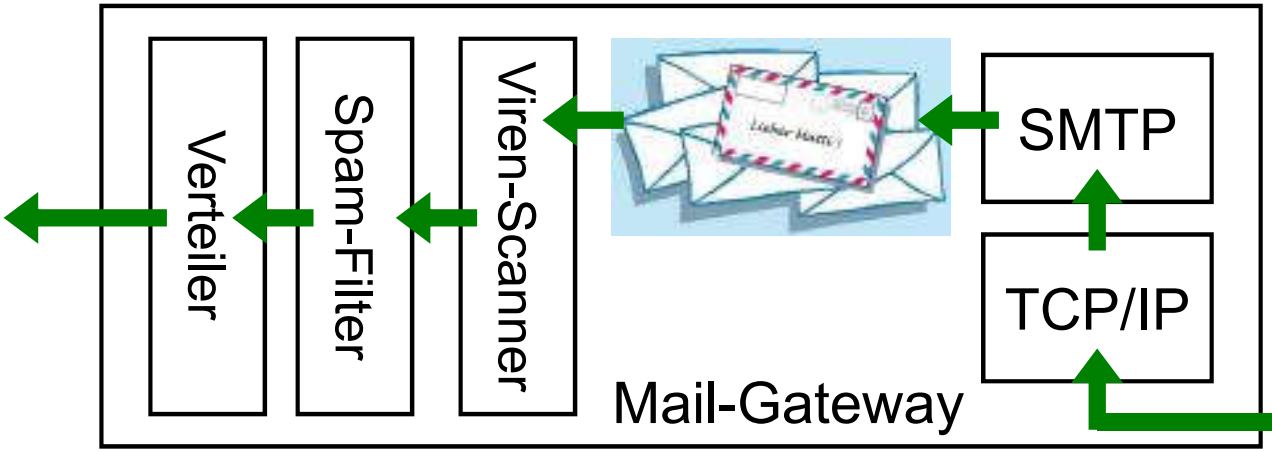
Vergleich

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

*restliche 3,9 % nicht zuordbar

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**

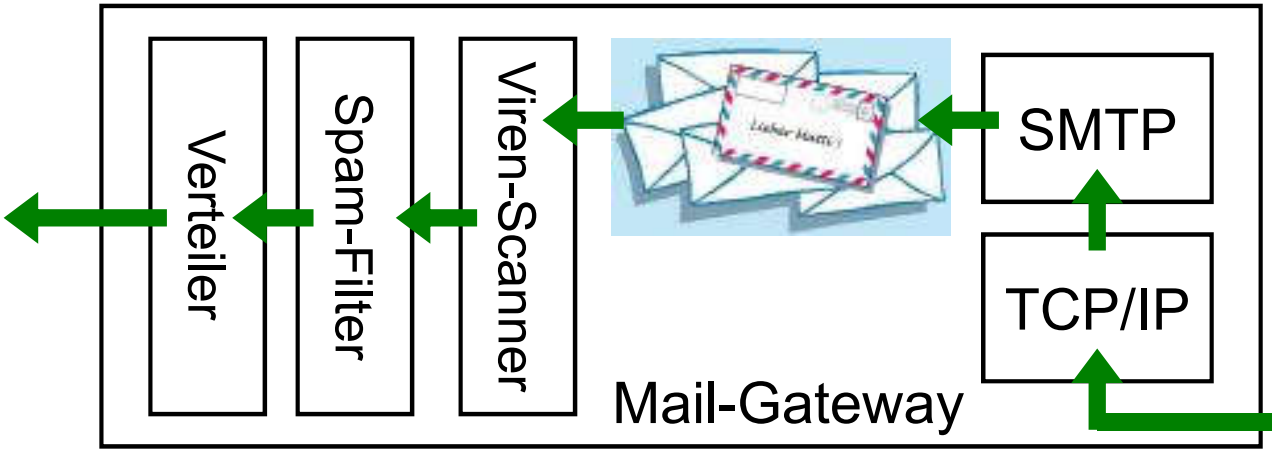


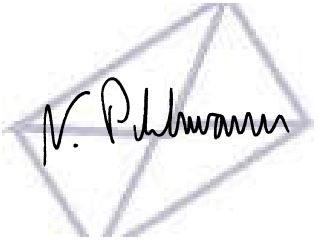
- **Verfahren:**
  - PGP/OpenPGP/GPG: 36,7%
  - S/MIME: 22,8%
  - Passphrase-gestützt: 3,8%

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

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

Sehr gering						Sehr hoch
☐	☐	☐	☐	X	☐	☐

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

Sehr gering					Sehr hoch
☐	☐	☐	☐	X	☐

Wie würden Sie die heutige Bedrohungslage (Spam) einschätzen?

Sehr gering						Sehr hoch
☐	☐	☐	☐	X	☐	☐

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

Sehr gering						Sehr hoch
☐	☐	☐	☐	X	☐	☐

Inhalt

- E-Mail Anwendung
- Umfrage „E-Mail Verlässlichkeit“
- **Einschätzung „Viren, Würmer, Trojaner, …“**
- Spam
- 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

Inhalt

- E-Mail Anwendung
- Umfrage „E-Mail Verlässlichkeit“
- Einschätzung „Viren, Würmer, Trojaner, …“
- **Spam**
- Zusammenfassung

Spam-Mails
→ Definition

- Spam ist eine **unerwünschte, für den Empfänger wert-, nutz- und sinnlose E-Mail**
- Internetjargon: **SPiced HAM** = Spam
- „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 wird in Massen versendet
  - Es gibt einen geschäftlichen Hintergrund
  - Denial of Service

Spam-Mails
→ Quellen von Spam

- **Spam-Server**
  → rückläufig (ca. 5 Mio. IP-Adressen in gängigen Blacklisten)
- **Missbrauchte/schlecht konfigurieret (Mail)-Server**
  → rückläufig (ca. 2,5 Mio. hijacked Mailserver)
- **Open Relays**
  → stabil (ca. 225.000 Server)
- **Open Proxies**
  → rückläufig (ca. 6,4 Mio. Hosts)
- **Unsichere CGI-Skripte (formmail)**
  → rückläufig (ca. 2,44 Mio. IP-Adressen)
- **Zombie PCs und Botnets**
  → auf dem Vormarsch
  (ca. 1 Mio. Zombies, pro Botnet bis zu 400.000 Zombies)
- **Mailserver der Provider**
  → kein großes Problem mehr

Spam-Mails
→ Motivation von Spam-Mails

- Spam-Mails kosten weniger als normale Werbepost.
- Die Kosten werden vom Anbieter zum Empfänger verschoben!
  - **Werbung, die nichts kostet, ist besonders interessant, wenn die wirtschaftliche Lage schlecht ist!**
- Das Internet ist ein **offenes System**, jeder kann jedem etwas senden.
- Der Dienst E-Mail muss **nicht** besonders **bezahlt werden.**

Schäden, die durch Spam-Mails auftreten
→ Überblick (1/2)

- **Arbeitszeitverlust**
  - Echtzeitsignalisierung, erkennen, aussortieren und löschen
- **Speichergebrauch**
  - von nicht gewünschten Werbe-Mails
- **Bandbreitenverbrauch**
  - von nicht gewünschten Werbe-Mails
- **Sicherheitsproblem**
  - Viren, Würmer, Trojaner

Schäden, die durch Spam-Mails auftreten
→ Überblick (2/2)

- **Mails-Server lahmlegen**
  - Rücklauf von fremden Spam-Mails
- **Reputation**
  - Spammer nutzen den Mail-Server eines Unternehmens (Pornographie, Gewalt, usw.)
- **Nutzbarkeit**
  - E-Mail ist wegen der sehr hohen Belastung nicht mehr nutzbar

Spam-Mails
→ Mechanismen zum Erkennen (1/2)

- **E-Mail-Kopfzeilen Analyse und Strukturanalyse**
  - Spam-Mails haben manipulierte Kontrollfelder (Absender, Route, ...)
  - Vergleich mit Standard (Microsoft, Lotus Notes, Netscape, ...)

- **Textanalyse durch gewichtete Wortlisten in Betreff und Nachrichtentext**
  - SEX, „Werden Sie reich“, ...
  - Gewichtungsalgorithmus, Schwellenwert, Heuristik, ... **(73%)**

- **Textanalyse mit statistischen Verfahren wie z.B. Content Recognition Engine (CORE) - (97%)**
  - flexibles Verfahren zur systematischen Erkennung von Inhalten
  - frei definierbare Kategorien (Spam-Mails, Newsletter, Business, usw.)

Spam-Mails
→ Mechanismen zum Erkennen (2/2)

- **Distributed Checksum Clearinghouse (DCC)**
  - jede Mail hat ein Prüfsumme (Fuzzy - unscharf)
  - Zählerstand im Clearinghouse
  - Schwellenwert
- **SpamNet**
  - ähnlich wie bei DCC, jedoch individuelle Klassifikation durch Endbenutzer
  - 3,99 US$ monatlich

Spam-Mails
→ Bewertung der Erkennungsmechanismen

- Die **Spam-Mails werden nach wie vor zum Zielsystem übertragen**, wodurch Bandbreitenverbrauch, Speicherverbrauch, Arbeitszeitverlust und damit auch Kosten entstehen!
- Auf dem Zielsystem werden sie dann z.B. im Betreff als Spam gekennzeichnet oder in "Spam"-Ordner einsortiert.
- Spam-Mails dürfen meist aber aus rechtlichen Gründen nicht automatisch gelöscht werden!
- Es wird in der Zukunft nie Erkennungssysteme geben, die Spam-Mails automatisch löschen können (**False Positive Rate - Problematik**)!
- Aus diesem Grund wird der **Aufwand** bei Erkennungsmechanismen für den Anwender **immer „zu groß“** sein!

Spam-Mails
→ Mechanismen zum Verhindern (1/2)

- **Absendererkennung und Blockierung der Absender per IP-Adresse und Name**
  - Problem sind die richtigen Sperrlisten (False Positive Rate)
  - Hier wird noch richtig geforscht!

- **Nutzung von Domain Name System zur Namensauflösung**
  - Überprüfung, ob die Adresse zum Domänennamen gehört
  - Die meisten Realisierungen haben diese Verfahren implementiert!
  - Kann von Spammern umgangen werden

- **Authentikation vor dem Versand**
  - Überprüfung, ob Client berechtigt ist, E-Mail zu senden
  - Die meisten Realisierungen haben diese Verfahren implementiert!
  - Muss in den Organisationseinheiten gepflegt werden!

Spam-Mails
→ Mechanismen zum Verhindern (2/2)

- **Realtime Blackhole List (RBL)**
  - Liste enthält alle ungeschützten Mailserver
  - Spam-Mails werden auch über geschützte Mailserver versendet

- **Whitelist**
  - List der legitimen Versender
  - Zusätzlich Verifikationssystem (antwortfähige Versender)

- **Sender Policy Framework (Sender Permitted From)**
  - Überprüfung von Domainen-Zugehörigkeit
  - Spam-Mails können nicht verhindert, aber dokumentiert werden

Spam-Mails
→ Bewertung von Verhinderungsmechanismen

- Mit den technischen **Mechanismen zur Vermeidung** von Spam-Mails kann ein **großer Effekt gegen Spam-Mails** erzielt werden.

- Aus diesem Grund sollen alle Unternehmen und Provider die beschriebenen technischen Mechanismen sinnvoll nutzen.

- Eine **vertrauenswürdige E-Mail-Infrastruktur** würde **Spam-Mails deutlich reduzieren!**

Weitere Methoden zur Verhinderung
→ Anwender (1/2)

- Zurückhaltung bei der Weitergabe der E-Mail-Adresse
- Verwendung von mehreren E-Mails-Adressen für unterschiedliche Zwecke (geschäftlich, private, ...)!
- Die E-Mail-Adresse in kein öffentliches Verzeichnis eintragen lassen!
- Nutzung von Dummy-Adressen, wo sinnvoll und möglich
- Immer lange E-Mail-Adressen verwenden
- Indirekte Darstellung von E-Mail-Adressen auf den Web-Seiten
- E-Mails gleichzeitig an mehrere, einander unbekannte Empfänger immer mit BCC versenden!

Weitere Methoden zur Verhinderung
→ Anwender (2/2)

- Nutzungsbedingungen und Datenschutzrichtlinien von Services „analysieren“, damit diese nicht legal die E-Mail-Adresse des Nutzers verkaufen können.
- Keine Spam-Mails öffnen (Sicherheitsproblem)
- Nie antworten, falls versehentlich geöffnet, damit die Spammer die Adresse nicht verifizieren können.
- **Nie kaufen**, damit sich Spam-Mails nicht lohnen!

Bewertung der Mechanismen, die jeder Anwender zur Verfügung hat

- Durch diese Maßnahmen können Spam-Mails für jedes Individuum (deren E-Mail-Adresse) sehr gut reduziert werden!
- Außerdem wird es den Spammern schwer gemacht daraus ein **lohneswertes Geschäft** zu machten!

Ausblick und Perspektiven
→ Spam-Mails: Forderungen

- **Erkennen von Spam-E-Mails, aber nicht um jeden Preis**
  - Mit dem Einsatz von Anti-Spam-Technologien können Spam-Mails erkannt werden, was **hilft,** mit dem Umgang von Spam-Mails besser klar zu kommen.
  - Dazu sollten aber in Zukunft **vermehrt Feedbackmechanismen** berücksichtigt werden, um viel bessere Ergebnisse zu erzielen.
- **Verhinderung von Spam-Mails in der Infrastruktur!**
  - Die Unternehmen und Provider sollen alles tun, um ihre MTAs und Mail-Clients gegen Mißbrauch zu schützen, damit die Spam-Mails so stark wie nur möglich schon in der Infrastruktur verhindert werden.
- **Bestrafung vorantreiben!**
  - Die Versendung von Spam-Mails muss international sehr hoch bestraft werden.

Inhalt

- E-Mail Anwendung
- Umfrage „E-Mail Verlässlichkeit“
- Einschätzung „Viren, Würmer, Trojaner, …“
- Spam
- **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, Diszipin, usw...).
- Wir sind selbst für die IT-Sicherheit verantwortlich!
- Wir brauen einen Viren- und Spam-Schutz, für die kontrollierte Annahme von E-Mails.

Fachhochschule Gelsenkirchen

Sicherheit im E-Mail-Verkehr (Spam)

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.