

Spam-Situation – Ergebnisse einer Umfrage

Christian Dietrich
christian.dietrich@informatik.fh-gelsenkirchen.de
Institut für Internet-Sicherheit
<http://www.internet-sicherheit.de>
Fachhochschule Gelsenkirchen



Inhalt

- Die Umfrage zum Thema E-Mail-Verlässlichkeit
- Spam – Zahlen und Fakten
- Anti-Spam-Mechanismen
- Ausblick

Die Umfrage – Ende 2004

- 116 Teilnehmer (148 Anmeldungen)
- Repräsentativ für
 - 40 Mio. E-Mail-Accounts
 - Monatl. E-Mail-Volumen von 2,3 Mrd. E-Mails (ca. 1/400 aller E-Mails weltweit)

Spam – relative Zahlen

- Relative Maxima für GbR & Einzelunternehmen, mögliche Gründe:
 - E-Mail-Harvester:
Große Unternehmen haben nicht die E-Mail-Adressen aller Angestellter auf den Webseiten verfügbar, sondern meist nur Kontakt-Adressen (info@..., contact@...)
 - Einzelunternehmer „müssen“ ihre E-Mail-Adresse auf die Webseite setzen
- Unternehmen mit vielen E-Mail-Accounts (AGs) anfälliger für DHA
- 61,5 % aller E-Mails sind Spam (Vergleich:
Brightmail (D) 43 %, Juli 2004;
MessageLabs (UK): 73 %)
- „Realer“ Wert vermutlich noch höher

Rechtsform	Spam-Rate
Aktiengesellschaft	69,9%
Behörde	20,4%
Gesellschaft mit beschränkter Haftung	64,0%
Hochschule	46,9%
ISP	61,1%
andere	42,1%
Durchschnitt	61,5%

E-Mails und schwarze Löcher

- Durchschnittlich ca. **16,5%** aller E-Mails mit nicht-existierender Empfänger-Adresse
- Maximum nach Branchen (ohne ISPs):
Finanzdienstleistungen (37 %)
- Ca. **36%** der Befragten weisen E-Mails mit nicht-existierenden Empfänger-Adressen bereits im SMTP-Dialog ab
- **11,5%** weisen nicht ab und senden keine NDNs

Anteil mit nicht existenter Empfänger-Adresse (in Prozent) nach Rechtsformen	
Rechtsform	Ergebnis
Aktiengesellschaft	33,6
Behörde	10,9
Gesellschaft mit beschränkter Haftung	6,3
Hochschule	9,3
ISP	45,0
andere	21,5
Gesamtergebnis	16,5

Anteil mit nicht existenter E-Mail-Empfänger Adresse (in Prozent) nach Branchen	
Branche	Ergebnis
Bildungsinstitution	10,0
Finanzdienstleistungen	37,0
Informationstechnologie	18,7
Öffentlicher Dienst	9,4
ISP	45,0
Industrie	4,5
Dienstleistungen	12,0
Gesamtergebnis	16,5

Anti-Spam-Mechanismen

- Am häufigsten eingesetzte Spam-Gegenmaßnahmen sind Header- und Wortanalyse sowie Heuristik und Blacklists
- 46,8 % nutzen Blacklist in Verbindungsaufbau oder Scoring
- 43 % nutzen Whitelist in Verbindungsaufbau oder Scoring
- 20,3 % setzen sowohl Black- als auch Whitelist in Verbindungsaufbau ein
- 12,9 % setzen sowohl Black- als auch Whitelist als Scoringquelle ein

Gegenmaßnahme	Ergebnis
Mittelwert von Blockieren von dynamischen IPs	20,3%
Mittelwert von Blockieren von dynamischen IPs (Inhalt)	15,2%
Mittelwert von Existenz der Empfänger-Adresse (Verbindungsaufbau)	29,1%
Mittelwert von Existenz der Empfänger-Adresse (Inhalt)	12,7%
Mittelwert von Blacklist (Verbindungsaufbau)	29,1%
Mittelwert von Blacklist (Inhalt)	32,9%
Mittelwert von Whitelist (Verbindungsaufbau)	29,1%
Mittelwert von Whitelist (Inhalt)	21,5%
Mittelwert von Greylist (Verbindungsaufbau)	10,1%
Mittelwert von Greylist (Inhalt)	7,6%
Mittelwert von Teergrube	7,6%
Mittelwert von Header-Analyse	48,1%
Mittelwert von Wortanalyse	58,2%
Mittelwert von Hash/Signatur	27,8%
Mittelwert von Frequenzmessungen des Kommunikationsverhaltens (Verbindungsaufbau)	7,6%
Mittelwert von Frequenzmessungen des Kommunikationsverhaltens (Inhalt)	3,8%
Mittelwert von Heuristik	31,6%

False Positive- und False Negative-Raten

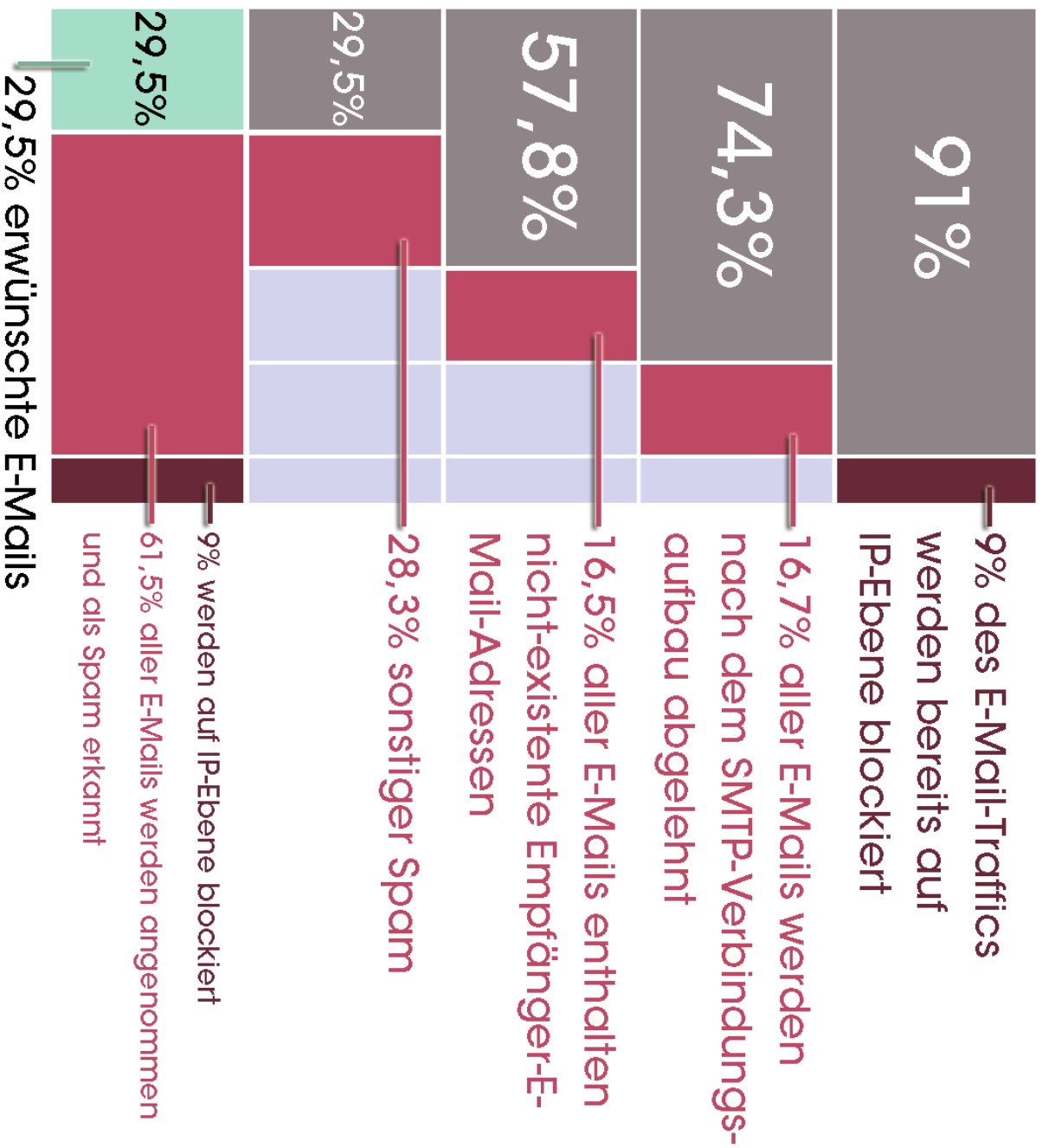
- Im Durchschnitt beträgt der Anteil an **False Negatives** 8,9%

Anteil an False Negatives (in Prozent)	
Rechtsform	Ergebnis
Aktiengesellschaft	3,1
Behörde	5,9
Gesellschaft mit beschränkter Haftung	17,6
Hochschule	5,5
ISP	4,0
andere	8,8
Gesamtergebnis	8,9

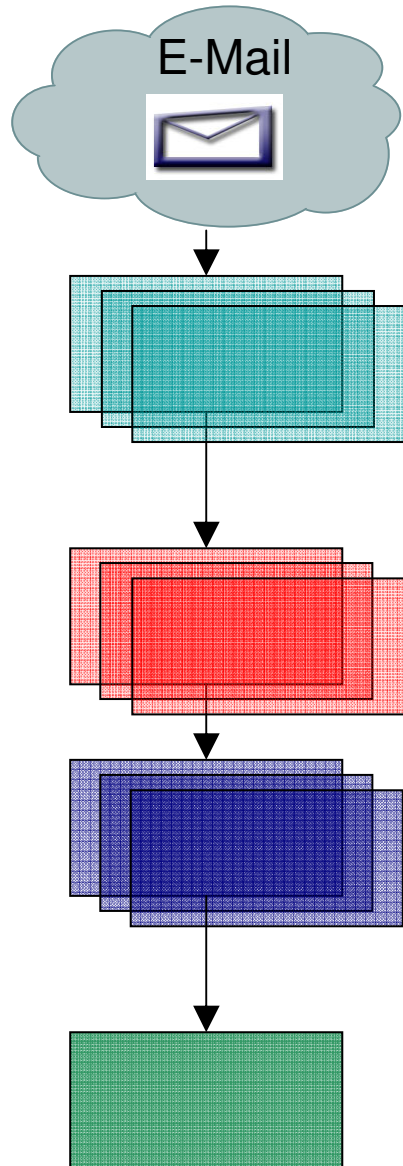
- Der Anteil an **False Positives** liegt bei 2,4%, teilweise Werte um 15%, Maximum: 20%
- Differenz:
GmbH: 3,7% ⇔ AGs: 1,1%

Anteil an False Positives (in Prozent)	
Rechtsform	Ergebnis
Aktiengesellschaft	1,1
Behörde	3,1
Gesellschaft mit beschränkter Haftung	3,7
Hochschule	0,0
ISP	1,5
andere	1,6
Gesamtergebnis	2,4

Spam-Blockierung / Spam-Raten



Das Ebenenmodell



Ext. E-Mail-Gateway / E-Mail-Proxy als Teil einer Firewall <ul style="list-style-type: none">▪ Checks auf IP-Ebene (IP-Adresse des einliefernden Computers)<ul style="list-style-type: none">▪ Blacklists (RBL, Dynamischer-IP-Bereich, OpenRelay, ...)▪ Reverse MX, SPF, DomainKeys, ...▪ Frequenzmessung (Anzahl Verbindungen / Zeit etc.)▪ Checks auf SMTP-Ebene<ul style="list-style-type: none">▪ Überprüfen der HELO-Angabe▪ Überprüfen der E-Mail-Adressen (Black-/White-/Greylist)▪ Existenz der Empfänger-E-Mail-Adresse (DB, Verzeichnisdienst)	1
Spam-Filter <ul style="list-style-type: none">▪ Checks auf Nachrichten-Ebene<ul style="list-style-type: none">▪ Untersuchung des E-Mail-Headers▪ Wortliste▪ Hash/Signatur	2
Viren-Filter <ul style="list-style-type: none">▪ Checkt Nachricht und Anhänge auf Virenbefall	3
Interner E-Mail-Server	

Ressourcenverbrauch

Fazit und Ausblick

- Mehr als 61,5% Spam
- Blockieren auf IP-Ebene
 - ressourcenschonend
 - derzeit noch nicht weit verbreitet (ca. 33%)
 - Erkennungsrate kann noch deutlich verbessert werden
- Blockieren dynamischer ISP-Dial-Up-IP-Adressen
- E-Mails mit nicht-existierendem Empfänger-Account bereits im SMTP-Dialog ablehnen
- Mechanismen zur Spam-Abwehr müssen etabliert werden!

Spam-Situation – Ergebnisse einer Umfrage

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

Christian Dietrich
christian.dietrich@informatik.fh-gelsenkirchen.de
Institut für Internet-Sicherheit
<http://www.internet-sicherheit.de>
Fachhochschule Gelsenkirchen

