E-Müll für dich

Wie E-Mails und ihr Missbrauch funktionieren

Ein Experimentalvortrag

Kepler-Seminar Vortrag, 12. März 2004

Jan Theofel

E·T·E·S
EDV-Systemhaus

Übersicht

- Einleitung, Definitionen
- Was ist eine E-Mail?
- Mailclients und -server
- Header lesen und verstehen
- Was ist SPAM?
- Spammer- und Viren-Techniken
- Strike back!
- Ausblick

Mein Bezug zu E-Mails

- Tägliche Nutzung . . .

Mein Bezug zu E-Mails

- Tägliche Nutzung . . .
- . . . ca. 100 – 200 „Nutzmails“ am Tag

Mein Bezug zu E-Mails

- Tägliche Nutzung . . .
- . . . ca. 100 – 200 „Nutzmails“ am Tag
- . . . ca. 600 – 800 Mailinglisten-Mails am Tag

Mein Bezug zu E-Mails

- Tägliche Nutzung . . .
- . . . ca. 100 – 200 „Nutzmails“ am Tag
- . . . ca. 600 – 800 Mailinglisten-Mails am Tag
- . . . früher bis zu 200 SPAM-Mails am Tag

Mein Bezug zu E-Mails

- Tägliche Nutzung . . .
- . . . ca. 100 – 200 „Nutzmails“ am Tag
- . . . ca. 600 – 800 Mailinglisten-Mails am Tag
- . . . früher bis zu 200 SPAM-Mails am Tag
- Administration von z. Z. 20 Mailservern

Mein Bezug zu E-Mails

- Tägliche Nutzung . . .
- . . . ca. 100 – 200 „Nutzmails“ am Tag
- . . . ca. 600 – 800 Mailinglisten-Mails am Tag
- . . . früher bis zu 200 SPAM-Mails am Tag
- Administration von z. Z. 20 Mailservern
- Aktive Teilnahme in postfix-user-Liste

Mein Bezug zu E-Mails

- Tägliche Nutzung . . .
- . . . ca. 100 – 200 „Nutzmails“ am Tag
- . . . ca. 600 – 800 Mailinglisten-Mails am Tag
- . . . früher bis zu 200 SPAM-Mails am Tag
- Administration von z. Z. 20 Mailservern
- Aktive Teilnahme in postfix-user-Liste
- Aktive Teilnahme in de.admin.net-abuse.mail

Mein Bezug zu E-Mails

- Tägliche Nutzung . . .
- . . . ca. 100 – 200 „Nutzmails“ am Tag
- . . . ca. 600 – 800 Mailinglisten-Mails am Tag
- . . . früher bis zu 200 SPAM-Mails am Tag
- Administration von z. Z. 20 Mailservern
- Aktive Teilnahme in postfix-user-Liste
- Aktive Teilnahme in de.admin.net-abuse.mail
- Massive eigene SPAM-Filter-Erfahrung

Definitionen

- IP = numerische Rechnerkennung

Definitionen

- IP = numerische Rechnerkennung
- Hostname / FQDN = namentliche Rechnerkennung

Definitionen

- IP = numerische Rechnerkennung
- Hostname / FQDN = namentliche Rechnerkennung
- DNS = Domain Name System

Definitionen

- IP = numerische Rechnerkennung
- Hostname / FQDN = namentliche Rechnerkennung
- DNS = Domain Name System
- RFC = Request for Comments

Was ist eine E-Mail?

- „Nur“ eine Textdatei! 

Was ist eine E-Mail?

- „Nur“ eine Textdatei! 
- Bereiche: Header und Body mit Signature

Was ist eine E-Mail?

- „Nur“ eine Textdatei! ↗
- Bereiche: Header und Body mit Signature
- Formatierte E-Mails sind HTML ↗

Was ist eine E-Mail?

- „Nur“ eine Textdatei! ↗
- Bereiche: Header und Body mit Signature
- Formatierte E-Mails sind HTML ↗
- Attachments sind ebenfalls Text ↗

Was ist eine E-Mail?

- „Nur“ eine Textdatei! ↗
- Bereiche: Header und Body mit Signature
- Formatierte E-Mails sind HTML ↗
- Attachments sind ebenfalls Text ↗
- Unnötiges Volumen bei HTML/Attachments

Was ist eine E-Mail?

- „Nur“ eine Textdatei! ↗
- Bereiche: Header und Body mit Signature
- Formatierte E-Mails sind HTML ↗
- Attachments sind ebenfalls Text ↗
- Unnötiges Volumen bei HTML/Attachments
- → Missbrauch des Textformats

Was ist eine E-Mail?

- „Nur“ eine Textdatei! ↗
- Bereiche: Header und Body mit Signature
- Formatierte E-Mails sind HTML ↗
- Attachments sind ebenfalls Text ↗
- Unnötiges Volumen bei HTML/Attachments
- → Missbrauch des Textformats
- Definiert in RFC 822 und RFC 2822

Der Weg einer E-Mail

- SMTP = Simple Mail Transport Protokoll

Der Weg einer E-Mail

- SMTP = Simple Mail Transport Protokoll
- Client-Server-Kommunikation 

Der Weg einer E-Mail

- SMTP = Simple Mail Transport Protokoll
- Client-Server-Kommunikation ↗
- Server-Server-Kommunikation

Der Weg einer E-Mail

- SMTP = Simple Mail Transport Protokoll
- Client-Server-Kommunikation
- Server-Server-Kommunikation
- Server-Client-Kommunikation POP3/IMAP

Der Weg einer E-Mail

- SMTP = Simple Mail Transport Protokoll
- Client-Server-Kommunikation ↗
- Server-Server-Kommunikation
- Server-Client-Kommunikation POP3/IMAP
- MX und Backup-MX ↗

Der Weg einer E-Mail

- SMTP = Simple Mail Transport Protokoll
- Client-Server-Kommunikation ↗
- Server-Server-Kommunikation
- Server-Client-Kommunikation POP3/IMAP
- MX und Backup-MX ↗
- Zuständigkeiten der Mailserver ↗

Der Weg einer E-Mail

- SMTP = Simple Mail Transport Protokoll
- Client-Server-Kommunikation ↗
- Server-Server-Kommunikation
- Server-Client-Kommunikation POP3/IMAP
- MX und Backup-MX ↗
- Zuständigkeiten der Mailserver ↗
- Definiert in RFC 821

Mailserver

- sendmail – der Urvater

Mailserver

- sendmail – der Urvater
- postfix, exim, qmail, . . . – die jungen Wilden

Mailserver

- sendmail – der Urvater
- postfix, exim, qmail, . . . – die jungen Wilden
- Exchange – der Ungeliebte

Mailserver

- sendmail – der Urvater
- postfix, exim, qmail, . . . – die jungen Wilden
- Exchange – der Ungeliebte
- Lotus Domino – der AW: Platzhirsch

Mailserver

- sendmail – der Urvater
- postfix, exim, qmail, . . . – die jungen Wilden
- Exchange – der Ungeliebte
- Lotus Domino – der AW: Platzhirsch
- Sonstige Kleinen – die Ahnungslosen

Mailclients

- mutt, pine, elm, . . . – die Gurus

Mailclients

- mutt, pine, elm, . . . – die Gurus
- Kmail & Co. – die grafischen Gurus

Mailclients

- mutt, pine, elm, . . . – die Gurus
- Kmail & Co. – die grafischen Gurus
- Outlook (Express) – der Störenfried

Mailclients

- mutt, pine, elm, . . . – die Gurus
- Kmail & Co. – die grafischen Gurus
- Outlook (Express) – der Störenfried
- Mozilla / Netscape – die Wollmilchsau

Mailclients

- mutt, pine, elm, . . . – die Gurus
- Kmail & Co. – die grafischen Gurus
- Outlook (Express) – der Störenfried
- Mozilla / Netscape – die Wollmilchsau
- Pegasus und The Bat – die Alternativen

Mailclients

- mutt, pine, elm, . . . – die Gurus
- Kmail & Co. – die grafischen Gurus
- Outlook (Express) – der Störenfried
- Mozilla / Netscape – die Wollmilchsau
- Pegasus und The Bat – die Alternativen
- Lotus Notes – der AW: Platzhirsch

Mailclients

- mutt, pine, elm, . . . – die Gurus
- Kmail & Co. – die grafischen Gurus
- Outlook (Express) – der Störenfried
- Mozilla / Netscape – die Wollmilchsau
- Pegasus und The Bat – die Alternativen
- Lotus Notes – der AW: Platzhirsch
- Sonstige Kleinen – die Ahnungslosen

Header-Zeilen

- Diverse Header-Zeilen ↗

Header-Zeilen

- Diverse Header-Zeilen ↗
- Recieved-Zeilen ↗

Header-Zeilen

- Diverse Header-Zeilen ↗
- Recieved-Zeilen ↗
- Gefälschte From: und To: Zeilen ↗

Header-Zeilen

- Diverse Header-Zeilen ↗
- Recieved-Zeilen ↗
- Gefälschte From: und To: Zeilen ↗
- Envelop-From und Envelop-To ↗

Header-Zeilen

- Diverse Header-Zeilen ↗
- Recieved-Zeilen ↗
- Gefälschte From: und To: Zeilen ↗
- Envelop-From und Envelop-To ↗
- Gefälschte Helo: Zeilen ↗

Header-Zeilen

- Diverse Header-Zeilen ↗
- Recieved-Zeilen ↗
- Gefälschte From: und To: Zeilen ↗
- Envelop-From und Envelop-To ↗
- Gefälschte Helo: Zeilen ↗
- Gefälschte Recieved: Zeilen ↗

Was ist SPAM?

SPAM kommt von SPAM

Was ist SPAM?

SPAM kommt von SPAM

UCE (unsolicited commercial email)
d. h. Unerwünschte Werbung per E-Mail
Auch bei „einmaligen“ Aktionen

Was ist SPAM?

SPAM kommt von SPAM

UCE (unsolicited commercial email)
d. h. Unerwünschte Werbung per E-Mail
Auch bei „einmaligen“ Aktionen

UBE (unsolicited bulk email)
d. h. Massen-E-Mails, Kettenbriefe, . . .

Was ist SPAM?

SPAM kommt von SPAM

UCE (unsolicited commercial email)
d. h. Unerwünschte Werbung per E-Mail
Auch bei „einmaligen“ Aktionen

UBE (unsolicited bulk email)
d. h. Massen-E-Mails, Kettenbriefe, . . .

SPAM ist lästig und teuer!

SPAM-Klassiker 1/2

- Make money fast (MMF)

SPAM-Klassiker 1/2

- Make money fast (MMF)
- Nigeria Connection (419) 

SPAM-Klassiker 1/2

- Make money fast (MMF)
- Nigeria Connection (419)
- Lotterie-Gewinne

SPAM-Klassiker 1/2

- Make money fast (MMF)
- Nigeria Connection (419)
- Lotterie-Gewinne
- Dialer (rückläufig)

SPAM-Klassiker 1/2

- Make money fast (MMF)
- Nigeria Connection (419)
- Lotterie-Gewinne
- Dialer (rückläufig)
- Schnellball-Systeme

SPAM-Klassiker 1/2

- Make money fast (MMF)
- Nigeria Connection (419) 
- Lotterie-Gewinne
- Dialer (rückläufig)
- Schnellball-Systeme
- Viagra, Penis-Verlängerungen, . . .

SPAM-Klassiker 2/2

- Fraud-Mails (Visa, eBay)

SPAM-Klassiker 2/2

- Fraud-Mails (Visa, eBay)
- Viren-/Wurm-Mails

SPAM-Klassiker 2/2

- Fraud-Mails (Visa, eBay)
- Viren-/Wurm-Mails
- Ketten-Mails

SPAM-Klassiker 2/2

- Fraud-Mails (Visa, eBay)
- Viren-/Wurm-Mails
- Ketten-Mails
- Hoax: Virenwarnungen

SPAM-Klassiker 2/2

- Fraud-Mails (Visa, eBay)
- Viren-/Wurm-Mails
- Ketten-Mails
- Hoax: Virenwarnungen
- Hoax: Spendenaufrufe

SPAM-Klassiker 2/2

- Fraud-Mails (Visa, eBay)
- Viren-/Wurm-Mails
- Ketten-Mails
- Hoax: Virenwarnungen
- Hoax: Spendenaufrufe
- Joe-Jobs

Spammer- und Virentechnik 1/2

- Harvester zum Adress-Sammeln

Spammer- und Virentechnik 1/2

- Harvester zum Adress-Sammeln
- Gefälschte Absender

Spammer- und Virentechnik 1/2

- Harvester zum Adress-Sammeln
- Gefälschte Absender
- Gefälschte HELOs

Spammer- und Virentechnik 1/2

- Harvester zum Adress-Sammeln
- Gefälschte Absender
- Gefälschte HELOs
- Gefälschte Recieved-Zeilen

Spammer- und Virentechnik 1/2

- Harvester zum Adress-Sammeln
- Gefälschte Absender
- Gefälschte HELOs
- Gefälschte Recieved-Zeilen
- Remove-URLs ↗

Spammer- und Virentechnik 1/2

- Harvester zum Adress-Sammeln
- Gefälschte Absender
- Gefälschte HELOs
- Gefälschte Recieved-Zeilen
- Remove-URLs 
- Remove-URLs mit automatischer Erkennung

Spammer- und Virentechnik 1/2

- Harvester zum Adress-Sammeln
- Gefälschte Absender
- Gefälschte HELOs
- Gefälschte Recieved-Zeilen
- Remove-URLs ↗
- Remove-URLs mit automatischer Erkennung
- Adress-Verifikation durch Bilder ↗

Spammer- und Virentechnik 2/2

- Text-Verstümmelung ↗

Spammer- und Virentechnik 2/2

- Text-Verstümmelung ↗
- URL-Verstümmelung

Spammer- und Virentechnik 2/2

- Text-Verstümmelung ↗
- URL-Verstümmelung
- Open Relays

Spammer- und Virentechnik 2/2

- Text-Verstümmelung
- URL-Verstümmelung
- Open Relays
- Offene Proxies

Spammer- und Virentechnik 2/2

- Text-Verstümmelung
- URL-Verstümmelung
- Open Relays
- Offene Proxies
- Social Engeniering

Spammer- und Virentechnik 2/2

- Text-Verstümmelung
- URL-Verstümmelung
- Open Relays
- Offene Proxies
- Social Engeniering
- Sicherheitslücken (Viren)

Spammer- und Virentechnik 2/2

- Text-Verstümmelung 
- URL-Verstümmelung
- Open Relays
- Offene Proxies
- Social Engeniering
- Sicherheitslücken (Viren)
- Missbrauchs-Netzwerke durch Viren

Strike back! - Die leichten Waffen

- Niemals „austragen“

Strike back! - Die leichten Waffen

- Niemals „austragen“
- SPAM-Filter

Strike back! - Die leichten Waffen

- Niemals „austragen“
- SPAM-Filter
- Blacklists

Strike back! - Die leichten Waffen

- Niemals „austragen“
- SPAM-Filter
- Blacklists
- Anrufen/Beschweren

Strike back! - Die leichten Waffen

- Niemals „austragen“
- SPAM-Filter
- Blacklists
- Anrufen/Beschweren
- T5F zustellen ↗

Strike back! - Die leichten Waffen

- Niemals „austragen“
- SPAM-Filter
- Blacklists
- Anrufen/Beschweren
- T5F zustellen ↗
- Remove-Skripte für Kollegen

Strike back! - Die leichten Waffen

- Niemals „austragen“
- SPAM-Filter
- Blacklists
- Anrufen/Beschweren
- T5F zustellen ↗
- Remove-Skripte für Kollegen
- Harvester mit Kollegen füttern

Strike back! - Die schweren Waffen

- Dialups blocken

Strike back! - Die schweren Waffen

- Dialups blocken
- Abuse-Mails verfassen

Strike back! - Die schweren Waffen

- Dialups blocken
- Abuse-Mails verfassen
- Kaufen! Kaufen!

Strike back! - Die schweren Waffen

- Dialups blocken
- Abuse-Mails verfassen
- Kaufen! Kaufen!
- DOS

Strike back! - Die schweren Waffen

- Dialups blocken
- Abuse-Mails verfassen
- Kaufen! Kaufen!
- DOS
- Spamtraps

Strike back! - Die schweren Waffen

- Dialups blocken
- Abuse-Mails verfassen
- Kaufen! Kaufen!
- DOS
- Spamtraps
- „Merkbefreiung“

Strike back! - Die schweren Waffen

- Dialups blocken
- Abuse-Mails verfassen
- Kaufen! Kaufen!
- DOS
- Spamtraps
- „Merkbefreiung“
- „Kleinbus“

Ausblick

- Der Kampf hat erst begonnen

Ausblick

- Der Kampf hat erst begonnen
- Schwellenländer

Ausblick

- Der Kampf hat erst begonnen
- Schwellenländer
- Zunahme von SPAM- und Virenaufkommen

Ausblick

- Der Kampf hat erst begonnen
- Schwellenländer
- Zunahme von SPAM- und Virenaufkommen
- Extrem Restriktive SPAM-Schutzmechnismen

Ausblick

- Der Kampf hat erst begonnen
- Schwellenländer
- Zunahme von SPAM- und Virenaufkommen
- Extrem Restriktive SPAM-Schutzmechnismen
- Missbrauch privater PCs wird steigen

Ausblick

- Der Kampf hat erst begonnen
- Schwellenländer
- Zunahme von SPAM- und Virenaufkommen
- Extrem Restriktive SPAM-Schutzmechnismen
- Missbrauch privater PCs wird steigen
- SMTP wird kurzfristig nicht abgelöst

Ausblick

- Der Kampf hat erst begonnen
- Schwellenländer
- Zunahme von SPAM- und Virenaufkommen
- Extrem Restriktive SPAM-Schutzmechnismen
- Missbrauch privater PCs wird steigen
- SMTP wird kurzfristig nicht abgelöst
- Pay-per-Mail Modelle sind eine Illusion

Ausblick

- Der Kampf hat erst begonnen
- Schwellenländer
- Zunahme von SPAM- und Virenaufkommen
- Extrem Restriktive SPAM-Schutzmechnismen
- Missbrauch privater PCs wird steigen
- SMTP wird kurzfristig nicht abgelöst
- Pay-per-Mail Modelle sind eine Illusion
- Probleme mit der E-Mail-Kommunikation

Ausblick

- Der Kampf hat erst begonnen
- Schwellenländer
- Zunahme von SPAM- und Virenaufkommen
- Extrem Restriktive SPAM-Schutzmechnismen
- Missbrauch privater PCs wird steigen
- SMTP wird kurzfristig nicht abgelöst
- Pay-per-Mail Modelle sind eine Illusion
- Probleme mit der E-Mail-Kommunikation
- Kosten werden steigen