Effiziente Bearbeitung von Abuse-Beschwerden

Wolfgang Hommel
Leibniz-Rechenzentrum München (LRZ)
hommel@lrz.de

Inhalt

- Kurze thematische Einführung
- Beschreibung der konkreten Problemstellung
- Vorstellung des am LRZ entwickelten „Abuse-Tools“
  - Systemarchitektur
  - Arbeiten mit dem graphischen Front-End
- Ausblick auf die zukünftige Entwicklung

Automatisierung bei IT-Security Incidents

- **Durchführen eines Angriffs**
  Kombination von Scannern und Exploits
  → je nach Art des Angriffs komplett automatisiert ✓

- **Erkennen eines Angriffs und Reaktion**
  Intrusion Detection Systeme
  → oft schon vollständig automatisiert ✓

- **Bearbeitung von Beschwerden über Angriffe**
  → musste bislang manuell erledigt werden ✗

Abuse-Beschwerden – warum und wie?

- Beschwerden als Reaktion auf Einbruchsversuche, Wurmattacken, (D)DoS, beleidigende E-Mails u.v.m.
- Sollen beim Administrator und nicht beim „Hacker“/ Verursacher landen.
- Ansprechpartner wird i.d.R. der WHOIS-Datenbank entnommen.

⇒ LRZ ist Betreiber und damit Ansprechpartner für das gesamte Münchener Wissenschaftsnetz (ca. 50.000 Endsysteme).

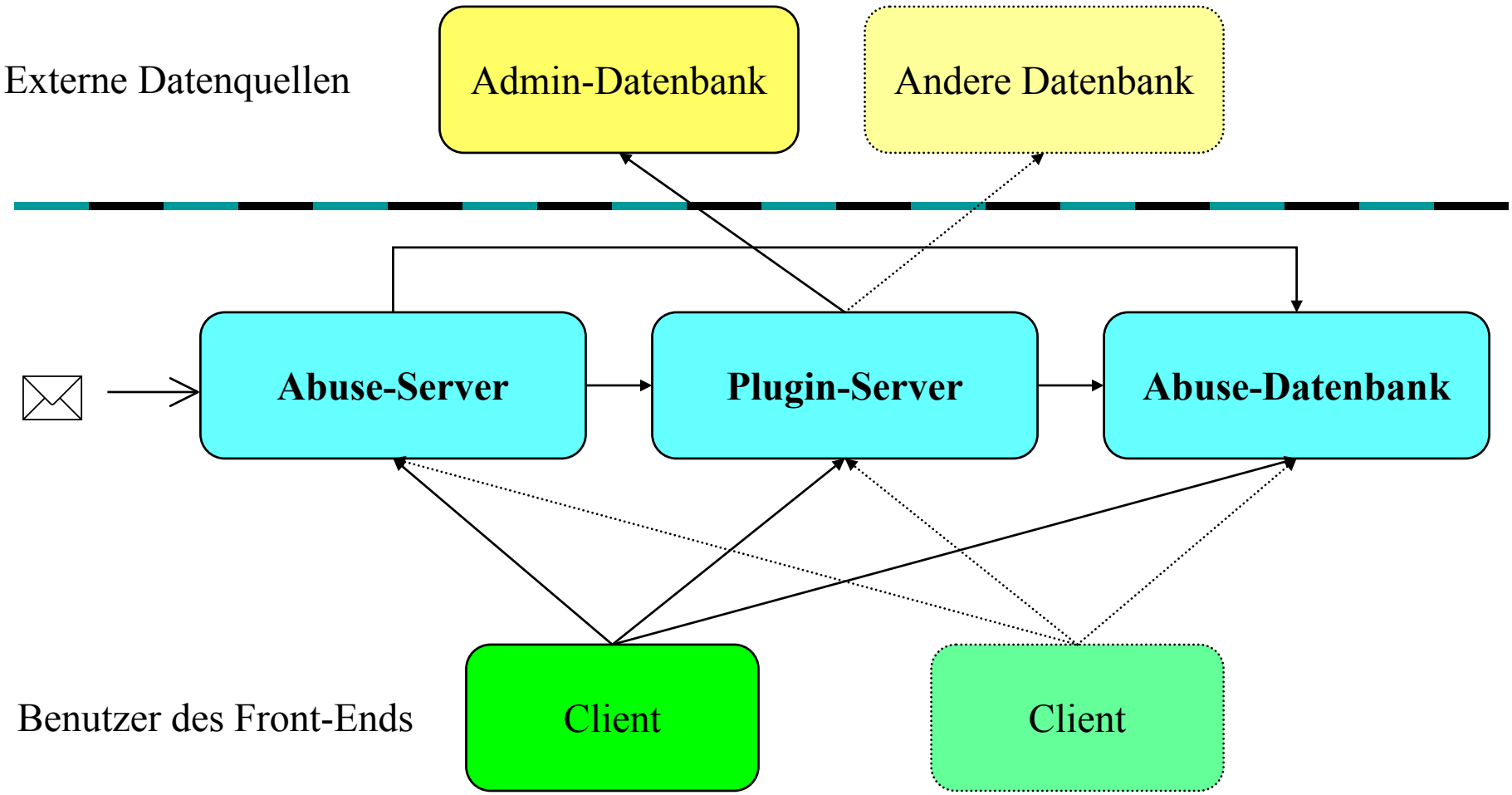
Reaktion auf Abuse-Beschwerden

- Einleiten von Sofortmaßnahmen
- Ermitteln des für den verursachenden Rechner verantwortlichen Administrators
- Kommentieren der Beschwerde und Weiterleiten an den/die zuständigen Verantwortlichen
- Antwort an den Beschwerdeführer
- Dokumentieren und Archivieren des Vorfalls

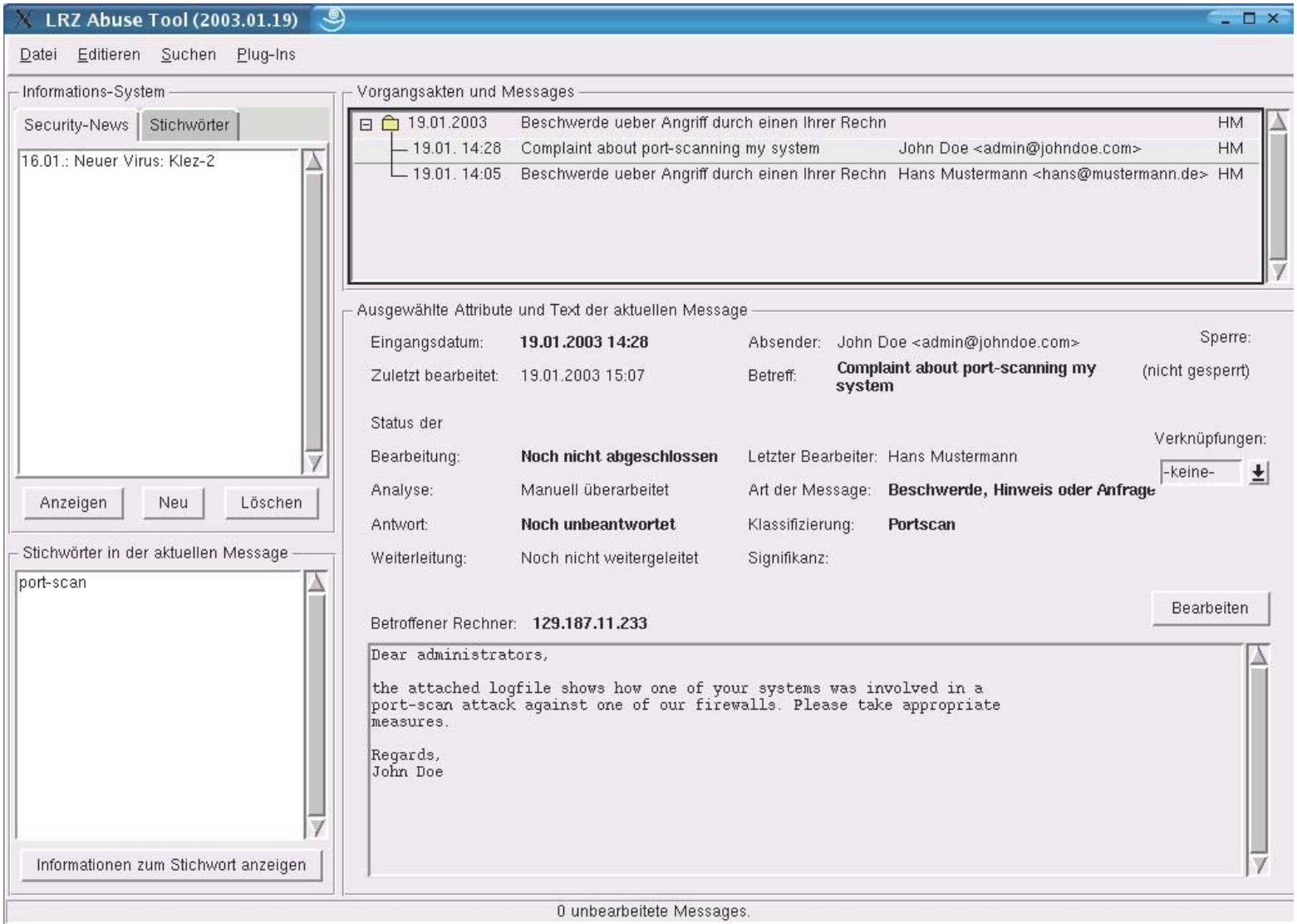
Optimierungsansätze

- Automatische Analyse eingehender E-Mails
- Automatische Beschaffung zur Bearbeitung notwendiger Informationen
- Textbaustein-System für ausgehende E-Mails
- Speicherung in einer „richtigen“ Datenbank
- Multi-User-Betrieb

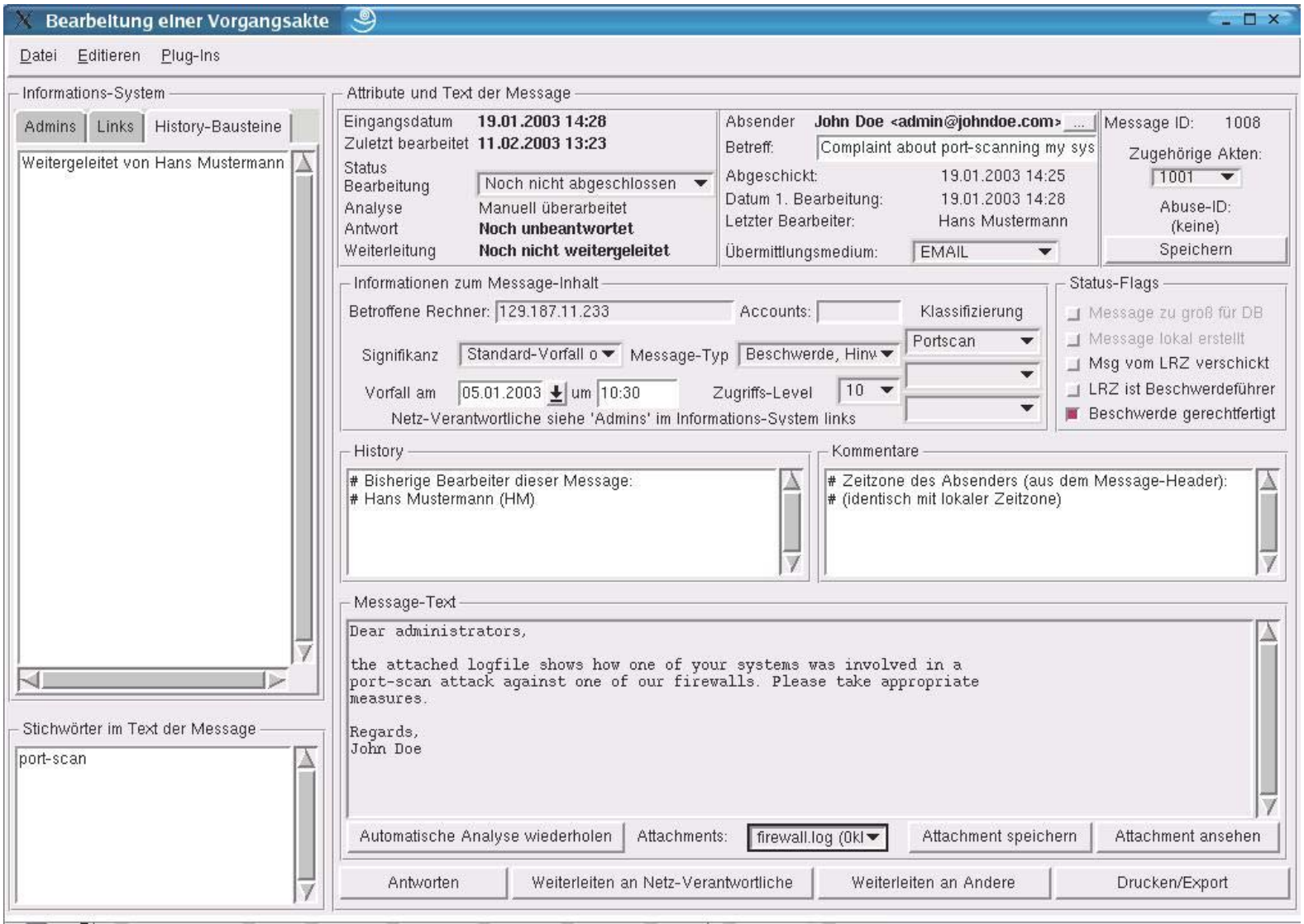
Architektur des LRZ-Abuse-Tools



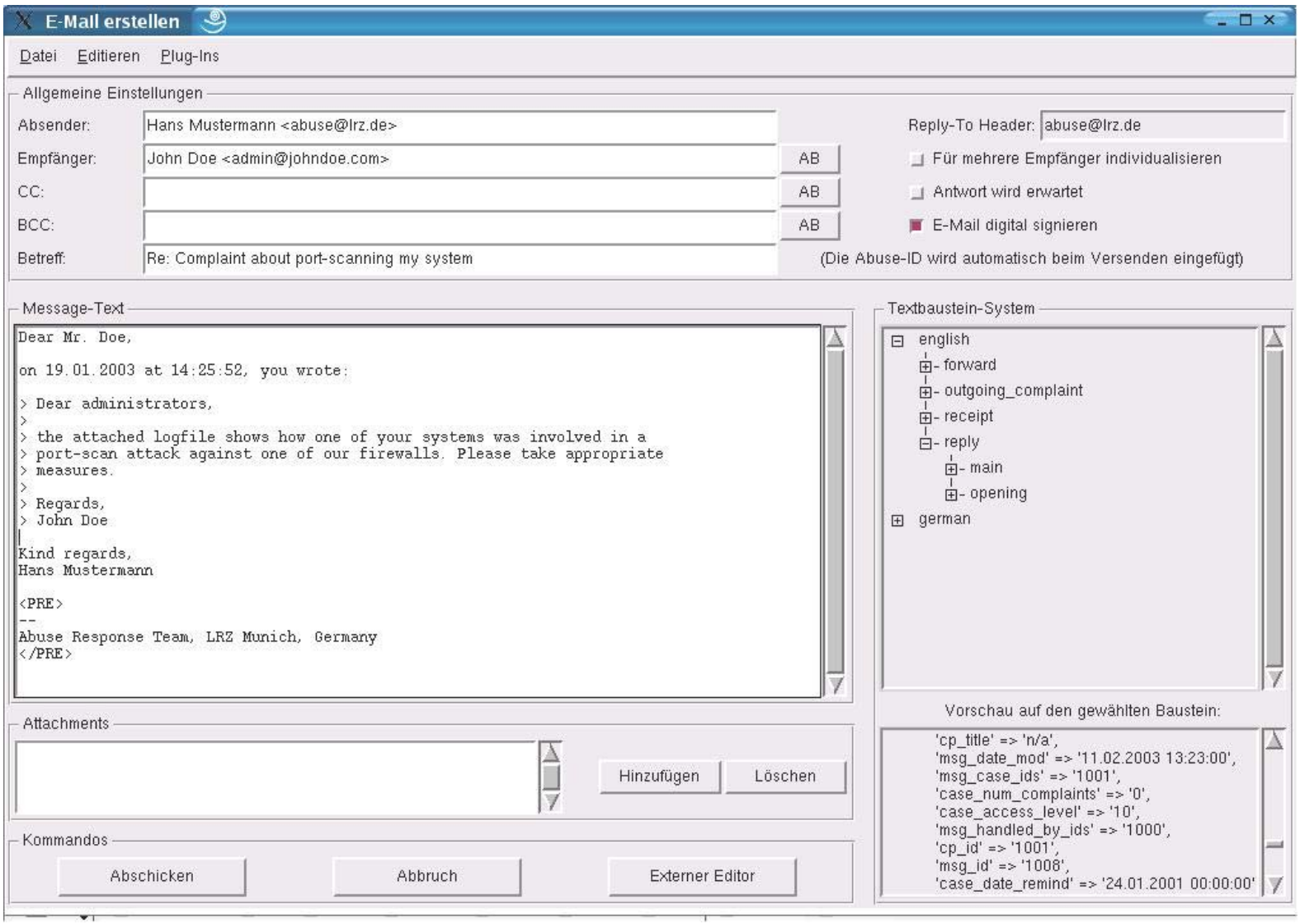
Graphische Benutzeroberfläche



Abuse-Tool GUI: Vorgangsbearbeitung



Abuse-Tool GUI: Erstellen von E-Mails



Ausblick

- Derzeitiger Stand:
  - Prototyp
  - Pläne für die Überführung in den Produktionsbetrieb
- Investition ins Customizing wichtig für spätere Zeitersparnis
- Weitere Verbesserungen des Bedienkomforts
- Integration in vorhandene Management-Werkzeuge