



Effiziente Bearbeitung von Abuse-Beschwerden

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

- ❑ 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

❑ **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, Wurmattaenken, (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).

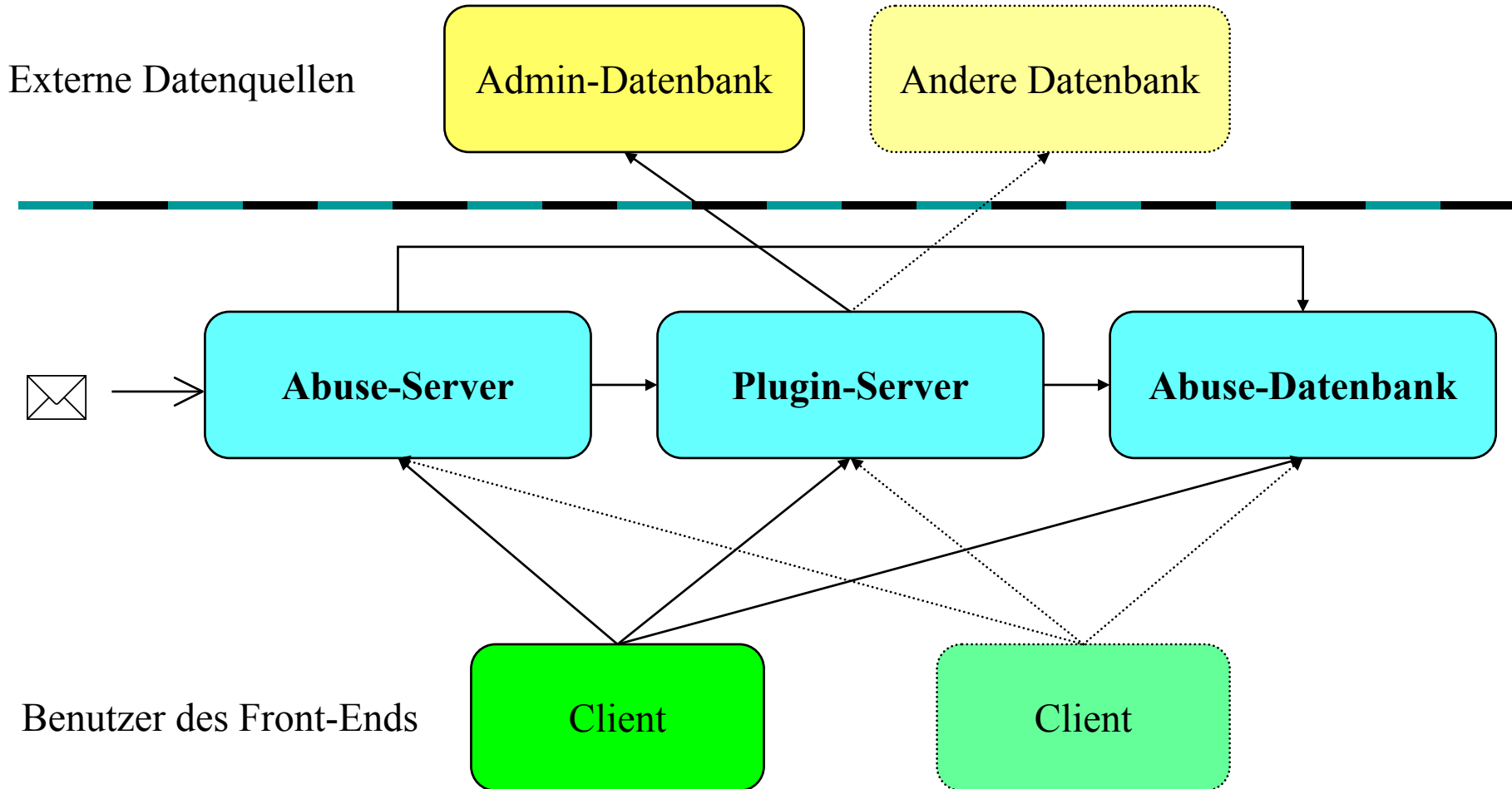
Reaktion auf Abuse-Beschwerden



- 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

- 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



The screenshot shows the LRZ Abuse Tool (2003.01.19) window. The interface is divided into several sections:

- Informations-System:** Contains a 'Security-News' tab and a 'Stichwörter' (Keywords) list with the entry '16.01.: Neuer Virus: Klez-2'. Below the list are buttons for 'Anzeigen', 'Neu', and 'Löschen'.
- Vorgangsaften und Messages:** A list of messages with columns for date, subject, sender, and status. The selected message is from 19.01.2003, subject 'Beschwerde ueber Angriff durch einen Ihrer Rechn', from John Doe <admin@johndoe.com>, with status 'HM'.
- Ausgewählte Attribute und Text der aktuellen Message:** Displays details for the selected message:
 - Eingangsdatum: 19.01.2003 14:28
 - Zuletzt bearbeitet: 19.01.2003 15:07
 - Absender: John Doe <admin@johndoe.com>
 - Betreff: **Complaint about port-scanning my system**
 - Sperre: (nicht gesperrt)
 - Status der Bearbeitung: **Noch nicht abgeschlossen**
 - Letzter Bearbeiter: Hans Mustermann
 - Analyse: Manuell überarbeitet
 - Art der Message: **Beschwerde, Hinweis oder Anfrage**
 - Antwort: **Noch unbeantwortet**
 - Klassifizierung: **Portscan**
 - Weiterleitung: Noch nicht weitergeleitet
 - Signifikanz:
 - Verknüpfungen: -keine-
 - Betroffener Rechner: **129.187.11.233**
- Stichwörter in der aktuellen Message:** A list containing 'port-scan'. Below it is a button 'Informationen zum Stichwort anzeigen'.
- Message Content:** A text area showing the message body:

Dear administrators,
the attached logfile shows how one of your systems was involved in a port-scan attack against one of our firewalls. Please take appropriate measures.
Regards,
John Doe

At the bottom of the window, it says '0 unbearbeitete Messages.'

Abuse-Tool GUI: Vorgangsbearbeitung



Bearbeitung einer Vorgangsakte

Datei Editieren Plug-Ins

Informations-System

Admins Links History-Bausteine

Weitergeleitet von Hans Mustermann

Attribute und Text der Message

Eingangsdatum **19.01.2003 14:28**
Zuletzt bearbeitet **11.02.2003 13:23**

Status
Bearbeitung **Noch nicht abgeschlossen**
Analyse **Manuell überarbeitet**
Antwort **Noch unbeantwortet**
Weiterleitung **Noch nicht weitergeleitet**

Absender **John Doe <admin@johndoe.com>**
Betreff: **Complaint about port-scanning my sys**
Abgeschickt: **19.01.2003 14:25**
Datum 1. Bearbeitung: **19.01.2003 14:28**
Letzter Bearbeiter: **Hans Mustermann**
Übermittlungsmedium: **EMAIL**

Message ID: **1008**
Zugehörige Akten: **1001**
Abuse-ID: **(keine)**
Speichern

Informationen zum Message-Inhalt

Betroffene Rechner: **129.187.11.233** Accounts: Klassifizierung **Portscan**

Signifikanz **Standard-Vorfall o** Message-Typ **Beschwerde, Hinw**

Vorfall am **05.01.2003** um **10:30** Zugriffs-Level **10**

Netz-Verantwortliche siehe 'Admins' im Informations-System links

Status-Flags

- Message zu groß für DB
- Message lokal erstellt
- Msg vom LRZ verschickt
- LRZ ist Beschwerdeführer
- Beschwerde gerechtfertigt

History

Bisherige Bearbeiter dieser Message:
Hans Mustermann (HM)

Kommentare

Zeitzone des Absenders (aus dem Message-Header):
(identisch mit lokaler Zeitzone)

Message-Text

Dear administrators,
the attached logfile shows how one of your systems was involved in a port-scan attack against one of our firewalls. Please take appropriate measures.

Regards,
John Doe

Stichwörter im Text der Message

port-scan

Automatische Analyse wiederholen Attachments: **firewall.log (0kl)** Attachment speichern Attachment ansehen

Antworten Weiterleiten an Netz-Verantwortliche Weiterleiten an Andere Drucken/Export

Abuse-Tool GUI: Erstellen von E-Mails



The screenshot shows the 'E-Mail erstellen' (Create Email) window of the Abuse-Tool GUI. The window has a menu bar with 'Datei', 'Editieren', and 'Plug-Ins'. Below the menu bar is the 'Allgemeine Einstellungen' (General Settings) section, which includes fields for 'Absender' (Sender: Hans Mustermann <abuse@lrz.de>), 'Empfänger' (Recipient: John Doe <admin@johndoe.com>), 'CC:', 'BCC:', and 'Betreff' (Subject: Re: Complaint about port-scanning my system). There are 'AB' buttons next to the recipient, CC, and BCC fields. To the right, there is a 'Reply-To Header' field (abuse@lrz.de) and three checkboxes: 'Für mehrere Empfänger individualisieren' (unchecked), 'Antwort wird erwartet' (unchecked), and 'E-Mail digital signieren' (checked). A note below these checkboxes states '(Die Abuse-ID wird automatisch beim Versenden eingefügt)'. The 'Message-Text' section contains a pre-formatted email body with a header, a quote of a previous message, and a signature block for Hans Mustermann from the Abuse Response Team, LRZ Munich, Germany. The 'Textbaustein-System' (Text Building Block System) section shows a tree view of templates, with 'english' selected and expanded to show sub-templates like 'forward', 'outgoing_complaint', 'receipt', 'reply', 'main', and 'opening'. The 'Attachments' section is empty. The 'Kommandos' (Commands) section at the bottom has buttons for 'Abschicken' (Send), 'Abbruch' (Cancel), and 'Externer Editor' (External Editor). A preview window at the bottom right shows the JSON metadata for the selected template.

```
'cp_title' => 'n/a',  
'msg_date_mod' => '11.02.2003 13:23:00',  
'msg_case_ids' => '1001',  
'case_num_complaints' => '0',  
'case_access_level' => '10',  
'msg_handled_by_ids' => '1000',  
'cp_id' => '1001',  
'msg_id' => '1008',  
'case_date_remind' => '24.01.2001 00:00:00'
```

- ❑ 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