Jens Nedon, Sandra Frings, Oliver Göbel (Hrsg.)

IT-Incident Management & IT-Forensics

Erste Tagung der Fachgruppe SIDAR der Gesellschaft für Informatik

24. – 25. November 2003 in Stuttgart, Deutschland

Gesellschaft für Informatik 2003

Lecture Notes in Informatics (LNI) - Proceedings
Series of the Gesellschaft für Informatik (GI)

Volume P-39

ISBN 3-88579-368-7
ISSN 1617-5468

Volume Editors
Jens Nedon
ConSecur GmbH
Schulze-Delitzsch-Strasse 2, D-49716 Meppen
Nedon@consecur.de
Sandra Frings
Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO
Nobelstraße 12, D-70569 Stuttgart
Sandra.Frings@iao.fhg.de
Oliver Göbel
RUS-CERT (Universität Stuttgart)
Breitscheidstr. 2, D-70174 Stuttgart
Goebel@CERT.Uni-Stuttgart.DE

printed by Köllen Druck+Verlag GmbH, Bonn

Effiziente Bearbeitung von Abuse-Beschwerden

Dr. Ernst Bötsch, Dr. Petra Eilfeld, Wolfgang Hommel

Leibniz-Rechenzentrum München
Barer Str. 21
D-80333 München
ernst.boetsch@lrz-muenchen.de,
petra.eilfeld@lrz-muenchen.de,
wolfgang.hommel@lrz-muenchen.de

Abstract: Über das Fehlverhalten der eigenen Rechner und Benutzer werden Organisationen üblicherweise durch eine Beschwerde an ihre Abuse-Adresse informiert. In diesem Artikel wird die Situation eines Hochschul-Rechenzentrums beschrieben, an dem die Bearbeitung derartiger Beschwerden bislang mangels dedizierter Software manuell erfolgte. Aufgrund der kontinuierlich steigenden Zahl derartiger Abuse-Fälle wurde der zur Bearbeitung notwendige Zeitaufwand jedoch inakzeptabel hoch. Abhilfe soll ein Tool schaffen, durch das der Prozess der Abuse-Bearbeitung so weit wie möglich automatisiert wird und das den Bearbeitern effiziente Hilfsmittel zur Verfügung stellt. Die Motivation für die Entwicklung dieses Werkzeugs, sein Konzept sowie die Implementierung eines ersten Prototyps werden vorgestellt.

1 Motivation

Das Leibniz-Rechenzentrum betreibt das Münchner Wissenschaftsnetz (MWN), ein regionales Netzwerk, an dem diverse Einrichtungen aus Forschung und Lehre angeschlossen sind. Entsprechend ist es auch für die IP-Adressen der Netzteilnehmer als Ansprechpartner für Missbrauchsfälle in der WHOIS-Datenbank[1] eingetragen.

Konsequenterweise gehen dort Beschwerden über alle Abuse-Fälle ein, deren auslösende Rechner oder Benutzer aus diesem regionalen Netz kommen. Das Spektrum dieser Beschwerden umfasst den Versand von Spam, Portscans, Hackversuche, DoS-Attacken, beleidigende E-Mails oder Newsgroup-Postings und vieles andere mehr. Die Anzahl der Beschwerden ist dabei in den letzten Monaten so stark gestiegen, dass die zu ihrer Bearbeitung erforderliche Arbeitszeit nicht mehr länger vernachlässigt werden konnte.

Da sich die Beschwerden fast ausschließlich auf Rechner beziehen, die nicht direkt vom Rechenzentrum administriert werden, erhöht sich der Aufwand lokal. Die Beschwerden müssen nämlich nicht nur beantwortet, sondern auch an die für die jeweiligen Rechner zuständigen Ansprechpartner weitergeleitet werden. Bei diesen handelt es sich in der

[1] siehe z.B. http://whois.arin.net/

Regel um Mitarbeiter der angeschlossenen Lehrstühle und Institute. Diese sind jedoch im Allgemeinen keine Informatiker, weshalb oft der Inhalt der Beschwerde für sie kommentiert und Lösungsmöglichkeiten für das zugrunde liegende Problem aufgezeigt werden müssen.

Sowohl das „Ausbeuten" von Sicherheitslücken auf der Seite der Angreifer als auch das Erkennen von Angriffen, kombiniert mit dem Versand von Beschwerden darüber, auf der Seite der Angegriffenen können bereits seit einiger Zeit automatisiert ablaufen. Die Bearbeitung solcher Beschwerden musste bisher jedoch mangels geeigneter Software manuell durchgeführt werden, wobei die folgenden Tätigkeiten die zeitaufwendigsten sind: das Auswerten einer Abuse-Beschwerde, die Einleitung eventuell notwendiger Sofortmaßnahmen wie das Abklemmen eines Rechners vom Netz im Falle akuter DoS-Attacken, die Ermittlung der für den Rechner Verantwortlichen, das Weiterleiten und Beantworten der Beschwerde sowie das Dokumentieren der Vorfälle und ihrer Bearbeitung.

Der Großteil der eingehenden Beschwerden bezieht sich auf Rechner bzw. IP-Adressen und nicht auf konkrete Personen. Bei den betroffenen Rechnern handelt es sich überwiegend um Systeme, die selbst kompromittiert worden sind. Meist ist die Ursache dafür eine Default-Installation oder eine (oft schon länger bekannte) Sicherheitslücke, die von den zuständigen Administratoren aus Mangel an Wissen und/oder Zeit nicht behoben wurde. Da kein Rückgang, sondern vielmehr ein weiteres kontinuierliches Ansteigen der Anzahl von Abuse-Fällen erwartet wurde, sollte ein Werkzeug konzipiert werden, das auf die Bearbeitung derartiger Beschwerden spezialisiert ist.

Die Ideen für dieses Tool, das daraus entwickelte Konzept und eine prototypische Implementierung werden im Folgenden vorgestellt.

2 Ansätze zur Automatisierung

Bei der großen Anzahl der Beschwerden ist es naheliegend, dass die Bearbeitung der einzelnen Fälle oftmals große Ähnlichkeiten aufweist. Deshalb wurde eine Tool-Unterstützung der am häufigsten anfallenden Tätigkeiten angestrebt:

- Aus dem Text der überwiegend per E-Mail eingehenden Beschwerden können die IP-Adressen und Host-Namen der lokal betroffenen Rechner extrahiert werden. Zu diesen können dann die zuständigen Ansprechpartner ermittelt werden. Im Falle des Leibniz-Rechenzentrums sind die Ansprechpartner in der Datenbank des Asset Managements eingetragen.

- Weiterhin können die Beschwerden nach Stichwörtern (z.B. „Spam" oder „Portscan") durchsucht werden, die Aufschluss darüber geben, um welche Art von Vorfall es sich handelt. Aus den so erkannten Vorfallstypen kann auch implizit eine Priorität für die Bearbeitung der Beschwerde abgeleitet werden. Beispielsweise wird man der Bearbeitung einer DoS-Beschwerde, die vielleicht noch akut anhält, eine höhere Priorität geben als der Bearbeitung einer

Spam-Beschwerde, die eventuell gar nicht gerechtfertigt ist, weil mit hoher Wahrscheinlichkeit gefälschte E-Mail-Header verwendet worden sind.

- Bei der Beantwortung von Beschwerden einerseits und bei der Weiterleitung an die zuständigen Verantwortlichen andererseits werden, je nach Vorfallstyp, oftmals inhaltlich ähnliche E-Mails verschickt. Beispielsweise wird den Beschwerdeführern bei Portscan-Vorfällen in der Regel mitgeteilt, dass der Vorfall bedauert wird und ihre Beschwerde an die zuständigen Verantwortlichen weitergeleitet worden ist. Die an die für den Rechner Verantwortlichen weitergeleitete Beschwerde wird dabei, in Abhängigkeit davon, was über deren Security-Kompetenz bekannt ist, mehr oder weniger ausführlich kommentiert, d.h. das Problem wird erläutert und mögliche Lösungswege werden aufgezeigt. Ein Texteditor oder E-Mail-Client, der die Übernahme einmal erstellter und immer wiederverwendeter Textbausteine in ausgehende E-Mails unterstützt, kann also wesentlich zu deren schneller Erstellung beitragen. Insbesondere könnte auch der gesamte Text der E-Mail von einem entsprechenden Tool vorgeschlagen werden, so dass er vom Bearbeiter nur noch bestätigt oder geringfügig modifiziert werden muss.

- Die Dokumentation der Bearbeitung der einzelnen Vorfälle, zu der beispielsweise die Erstellung einer Bearbeitungs-Historie gehört, kann durch eine automatische Protokollierung der durchgeführten Schritte verbessert werden. Die gesamte Korrespondenz und die zugehörigen Meta-Informationen können in einer Datenbank gespeichert und auf diese Weise effizient verwaltet werden.

Bereits diese Basisanforderungen legen nahe, dass für eine effizientere Abuse-Bearbeitung dedizierte Software notwendig ist, beispielsweise ein E-Mail-Client mit entsprechender Zusatzfunktionalität. Weitere Anforderungen, die über die reine Automatisierung der bisher manuell durchgeführten Tätigkeiten hinausgehen, werden im nächsten Abschnitt vorgestellt.

3 Workflow-Management

Bisher erfolgte die manuelle Abuse-Bearbeitung durch eine einzige Person, die das *abuse*-Postfach verwaltete. Langfristig ist es jedoch zwingend notwendig, dass neu eingehende Beschwerden von mehreren Abuse-Bearbeitern, i.A. parallel abgearbeitet werden können. Hierbei ist zu berücksichtigen, dass nicht alle Abuse-Bearbeiter jeden Fall bearbeiten oder einsehen dürfen. Beispielsweise ist es denkbar, dass studentische Hilfskräfte für die Bearbeitung von Beschwerden über Spam und Portscans eingesetzt werden; sie sollen jedoch keinen Zugriff auf Fälle mit möglicherweise strafrechtlich relevantem Inhalt haben. Hierzu gehören Anfragen von Ermittlungsbehörden, die bislang jedoch ausschließlich postalisch oder per Fax eingegangen sind; eine Möglichkeit, solche Anfragen in das Abuse-System zu integrieren, ist also ebenfalls notwendig.

Die Verwaltung der Vorfälle wird mittels Akten realisiert. Dabei enthält eine Akte alle zu einem Vorfall ein- und ausgehenden E-Mails sowie dazugehörige Meta-

Informationen. Um die Zuordnung von Antworten zu versandten E-Mails zu erleichtern, werden im „Betreff“ so genannte Abuse-IDs eingetragen, die ähnlich der Nummerierung von DFN-CERT Advisories funktionieren. Geht eine Antwort ein, bei der im „Betreff“ die Abuse-ID erhalten geblieben ist, so kann sie einfach ihrer entsprechenden Akte zugeordnet werden. Jede Abuse-ID darf dabei selbstverständlich nur ein einziges Mal vergeben werden. Eine simple Durchnummerierung ist jedoch unerwünscht, weil dadurch Rückschlüsse auf die Anzahl der bearbeiteten Missbrauchsfälle möglich wären. Ein einfacher Algorithmus, der einmalige Abuse-IDs aus dem aktuellen Jahr, Monat und Zufalls-Elementen bestimmt, sorgt für Abhilfe, indem er die Überprüfung der Eindeutigkeit vereinfacht.

In einigen Fällen wird von den Verantwortlichen, an die Beschwerden weitergeleitet werden, eine Antwort oder Stellungnahme erwartet; da die Bearbeitung von Abuse-Fällen aber bei diesen oft niedrige Priorität hat, kann es Tage oder gar Wochen dauern, bis die Antwort eintrifft. Das Abuse-System unterstützt deshalb ein Wiedervorlage-System, mit dessen Hilfe die Bearbeiter auf Wunsch einmalig oder periodisch an wichtige, noch nicht abgeschlossene Fälle erinnert werden können. Alle Abuse-Bearbeiter sind zu diesem Zweck in einem E-Mail-Verteiler zusammengefasst, bei dem jedoch sichergestellt wird, dass jeder Bearbeiter nur E-Mails über Vorfälle bekommt, auf die er auch zugreifen darf.

Optional können Bearbeiter auch angeben, dass sie per E-Mail über neu eingehende Beschwerden informiert werden möchten. In diesem Fall erhalten sie die ursprüngliche Beschwerde-E-Mail, angereichert mit den Ergebnissen der vom Abuse-System durchgeführten automatischen Analyse.

In einigen Fällen können die Abuse-Bearbeiter einen Fall nicht alleine bearbeiten, beispielsweise wenn Beschwerden über IP-Adressen eingehen, die gar nicht vergeben worden sind, also der Verdacht auf Spoofing vorliegt; der entsprechende verursachende Rechner muss dann erst von Netz-Spezialisten mit Hilfe einer „Fangschaltung” identifiziert werden. Entsprechend sind im Abuse-System auch Möglichkeiten dafür vorgesehen, die Bearbeitung eines Falles temporär an andere Bearbeiter zu übergeben und die Korrespondenz mit Experten anderer Abteilungen in der Akte des jeweiligen Vorfalls festzuhalten.

Neben den Beschwerden, die von externen Organisationen eingehen, gibt es auch noch eine Reihe intern erkannter Verstöße gegen die Nutzungsordnung. Zum Beispiel werden nicht selten lokal kompromittierte Rechner, auf denen FTP-Server mit illegalen Inhalten laufen, anhand von Auffälligkeiten in der Netzverkehrsstatistik ausfindig gemacht. An die Verantwortlichen dieser Rechner werden dann entsprechende Beschwerden verschickt. Häufig wird auch der betroffene Rechner sofort vom Netz abgeklemmt, bis das Problem behoben ist. Diese Tätigkeit wurde bisher von den Netz-Administratoren selbständig und unabhängig von der regulären Abuse-Bearbeitung durchgeführt. Das Abuse-System sieht jedoch entsprechende Schnittstellen vor, über die die Bearbeitung beider Arten von Missbrauchsfällen, d.h. der extern und intern erkannten, vereinheitlicht werden kann.

Bereits diese unvollständige Liste von Anforderungen an ein dediziertesWerkzeug zur Bearbeitung von Abuse-Fällen zeigt, dass es sich dabei um ein komplexes Software-

System handelt, das eine Reihe verschiedenster Funktionen unter einer einheitlichen Oberfläche zur Verfügung stellen muss. Um die Entstehung eines „quick & dirty" Tools zu verhindern, wurden die Konzeption und die Implementierung des „Abuse-Tools" als Diplomarbeit ausgeschrieben. Das Resultat ist ein offenes und erweiterbares Abuse-System, dessen Konzept und Einzelkomponenten in den folgenden Abschnitten vorgestellt werden.

4 Überblick über das Abuse-System

Konzeptionell besteht das gesamte System derzeit aus zwei Servern und beliebig vielen Clients, die im Folgenden noch näher erläutert werden:

- Die Abuse-Bearbeiter arbeiten an den Abuse-Clients mit einer graphischen Benutzeroberfläche, mit deren Hilfe die effiziente Verwaltung, Bearbeitung und statistische Auswertung von Missbrauchsfällen realisiert wird.

- Der Abuse-Server nimmt neu eingehende E-Mails entgegen, unterzieht diese einer automatischen Analyse und verwaltet einen E-Mail-Verteiler, in den alle Abuse-Bearbeiter eingetragen sind. Ferner laufen hier Wartungswerkzeuge und ein Datenbankmanagementsystem, in dem alle Abuse-Fälle samt Meta-Informationen abgelegt werden. Alternativ kann auch ein bereits vorhandenes anderes DMBS eingesetzt werden.

- Im Plugin-Server sind alle Funktionalitäten gekapselt, die entweder speziell auf die Infrastruktur des Rechenzentrums ausgelegt sind oder besondere Privilegien erfordern. Ein in Beispiel des betrachteten Rechenzentrums implementierter Dienst ist die Ermittlung der Verantwortlichen, an die eine Beschwerde weitergeleitet werden muss, aus der Datenbank des lokalen Asset Managements.

Die strikte Trennung zwischen Abuse- und Plugin-Server erhöht die Portabilität des Abuse-Systems – im Idealfall muss bei der Verwendung des Abuse-Tools in einer anderen Organisation nur die Implementierung des Plugin-Servers entsprechend angepasst werden.

Abbildung 4.1 gibt einen groben Überblick über die Komponenten des Abuse-Systems. Die einzelnen Komponenten haben die folgenden Aufgaben:

- Der Input-Handler nimmt E-Mails entgegen und verfügt auch über eine Schnittstelle für die manuelle Eingabe von Beschwerden.

- Der Message-Analyzer führt eine automatische Analyse neu eingegangener Beschwerden durch, extrahiert beispielsweise gefundene IP-Adressen und bestimmt mit Hilfe des Plugin-Servers die entsprechenden Verantwortlichen.

- Der Storage-Mediator sorgt für die transparente Anbindung an das verwendete Datenbankmanagementsystem.

- Das Maintenance-Tool kümmert sich um periodisch anfallende Wartungstätigkeiten, führt die Wiedervorlage-Funktion aus und kann vom Abuse-Administrator zur Verwaltung der Accounts der Abuse-Bearbeiter eingesetzt werden.

- Das Mail-Interface dient zum Versand von E-Mails. Es beinhaltet inbesondere auch die E-Mail-Verteiler-Funktionalität, die beispielsweise gewährleistet, dass nur diejenigen Abuse-Bearbeiter über einen Fall informiert werden, die auch entsprechende Zugriffsrechte darauf haben.

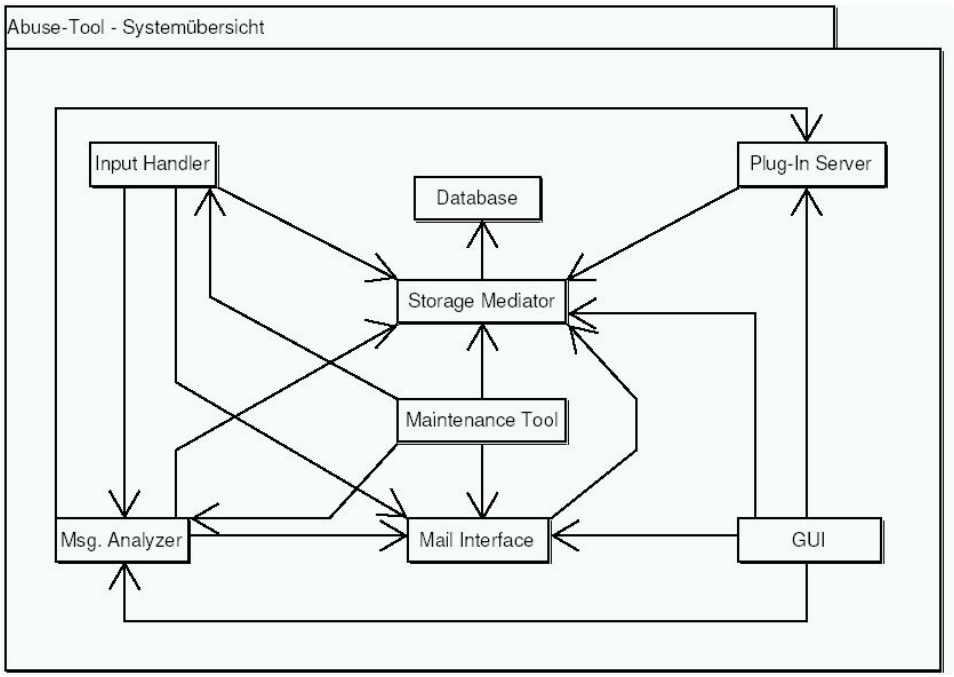

Abbildung 4.1: Die Komponenten des Abuse-Systems

- Der Plugin-Server stellt verschiedene Dienste bereit, die zur Bearbeitung von Missbrauchsfällen notwendig sind, beispielsweise das Durchführen eines Portscans zur Diagnose wahrscheinlich kompromittierter Rechner.

- Die graphische Benutzeroberfläche ist die interaktive Schnittstelle zum Abuse-System. Sie ermöglicht im Wesentlichen

  - die Verwaltung der eingegangenen und versandten E-Mails samt ihrer Akten,

  - das manuelle Einbringen neuer Fälle, z.B. durch Anfertigen des Protokolls eines Telefonats,

- das Bearbeiten einzelner Fälle, beispielsweise das Editieren der Meta-Informationen,

- das Erstellen neuer E-Mails bzw. das Beantworten oder Weiterleiten eingegangener E-Mails. In diesen integrierten E-Mail-Client ist insbesondere auch das bereits erwähnte Textbaustein-System eingebunden,

- den Zugriff auf die vom Plugin-Server angebotenen Dienste sowie Such- und Statistikfunktionen.

Die Funktionsweise dieser Komponenten wird im folgenden Abschnitt näher erläutert.

5 Komponenten des Abuse-Systems

Die Spezifikation der einzelnen Komponenten bildet den Schwerpunkt des Konzepts des Abuse-Systems; ihre Funktionalität und Vorgehensweise kann hier nur kurz angerissen werden. Bei Interesse kann das gesamte Konzept gerne zur Verfügung gestellt werden.

5.1 Input-Handler

Der *Input-Handler* dient der Aufnahme neuer Korrespondenz in das Abuse-System. Es handelt sich dabei um eine hybride Komponente, die sowohl neu eingehende E-Mails entgegennehmen kann als auch als Kommandozeilen-Tool und als API zur Verfügung steht, das von anderen Programmen verwendet werden kann. Seine Aufgabe ist die zuverlässige Speicherung der eingehenden Nachrichten in der Datenbank; ist diese beispielsweise nicht erreichbar, wenn eine neue E-Mail eingeht, so wird sie entsprechend zwischengepuffert. Bei lokal ins System eingebrachten Nachrichten können verschiedene Attribute wie beispielsweise die Zugriffsrechte vorgegeben werden. Bei über das Internet eingehenden E-Mails werden vom Administrator vorgegebene Defaultwerte dafür verwendet. Sofern nicht anders gewünscht, stößt der *Input-Handler* den nachfolgend beschriebenen *Message-Analyzer* an.

5.2 Message-Analyzer

Der *Message-Analyzer* gehört zu den umfangreichsten Komponenten des Systems. Seine Aufgaben umfassen

- die Nachbearbeitung der vom Input-Handler gelieferten Rohdaten. Bei E-Mails mit Attachments werden letztere beispielsweise dekodiert und aus Effizienzgründen in einer getrennten Datenbanktabelle abgelegt, so dass zum Beispiel eine Volltext-Suche über alle in der Datenbank gespeicherten E-Mails nicht durch MIME-kodierte Attachments verlangsamt wird.

- die Extraktion von Meta-Informationen, die mindestens aus der Auswertung der E-Mail-Header besteht:

- Informationen über die Absender von Beschwerden werden im globalen Adressbuch des Abuse-Systems gespeichert. Ist ein Absender bisher noch nicht bekannt, werden aus seiner E-Mail-Adresse Voreinstellungen für das Textbaustein-System ermittelt.

- Kommt die E-Mail von einer .de-Domain, so wird beispielsweise „Deutsch" als gewünschte Sprache für eine Antwort angenommen.

- Weitere Informationen können durch die Suche nach beliebig vorgebbaren Schlüsselwörtern sowie nach lokalen IP-Adressen gefunden werden. Ein Auftreten von Schlüsselwörtern führt zur automatischen Klassifizierung des Vorfallstyps und daraus zu einer impliziten Ableitung der Bearbeitungspriorität. Zu gefundenen IP-Adressen werden die Verantwortlichen ermittelt.

- Die Zuordnung der Nachricht zu einer Akte. Enthält der Betreff einer eingehenden E-Mail beispielsweise eine der bereits erwähnten Abuse-IDs, so fällt diese Zuordnung leicht. Andernfalls wird versucht, die Zuordnung anhand gefundener IPAdressen durchzuführen. Es kommt manchmal vor, dass zu einem kompromittierten Rechner in kurzen Zeitabständen mehrere Beschwerden unabhängig voneinander eintreffen; diese sollen dann in einer einzigen Akte zusammengefasst werden.

- Für den Fall, dass es sich um lokal erzeugte Nachrichten handelt, die Bearbeitung eventuell vorhandener besonderer Steuerbefehle. Hierbei steht ein Satz von Befehlen zur Verfügung, die das Ergebnis der automatischen Analyse vorwegnehmen und bestimmte Aktionen anstoßen können, wenn die Abuse-Bearbeiter bereits vorgeben wollen, was mit der Nachricht geschehen soll. Beispiele hierfür sind: „lege eine neue Akte für diese Nachricht an" und „trage als Meta-Information ein, dass es sich bei dieser Nachricht um ein abgetipptes Fax handelt". Entsprechende Steuerbefehle werden beispielsweise bei der Eingabe neuer Beschwerden über das Client-GUI automatisch erzeugt.

- Für den Fall, dass vom Absender der Beschwerde eine Empfangsbestätigung gewünscht wird und dies vom Abuse-Administrator erlaubt worden ist, den automatischen Versand einer entsprechenden E-Mail.

- Die Benachrichtigung der Abuse-Bearbeiter über die neu eingegangene Nachricht. Hierzu wird eine E-Mail verschickt, die neben dem ursprünglichen Nachrichtentext auch das Ergebnis der automatischen Analyse beinhaltet.

Nachdem die initiale Bearbeitung neu eingegangener Nachrichten durch *Input-Handler* und *Message-Analyzer* abgeschlossen ist, ist der nächste Schritt im imWorkflow die interaktive Bearbeitung des Falls durch einen Abuse-Bearbeiter.

5.3 Storage-Mediator

Aufgabe des *Storage-Mediators* ist es, eine einheitliche Schnittstelle für die anderen Komponenten des Abuse-Systems zu einem relationalen Datenbankmanagementsystem anzubieten. Oberstes Ziel ist hierbei die Transparenz des konkret eingesetzten RDBMS. Beispielsweise verwenden viele RDBMS unterschiedliche SQL-Dialekte: in einigen arbeitet der String-Vergleichsoperator `like` case-sensitive, in anderen case-insensitive. Ferner wird das RDBMS zum Beispiel für die Vergabe von Zeitstempeln für die automatisch erstellte Bearbeitungs-Historie von Vorfallsakten eingesetzt. Der entsprechende SQL-Befehl hierfür lautet, je nach RDBMS, zum Beispiel „`select sysdate from dual`" oder „`select now()`". Der *Storage-Mediator* ist also dafür verantwortlich, die in einer vorgegebenen SQL-Variante gestellten Anfragen in den SQL-Dialekt des eingesetzten RDMBS zu übersetzen.

5.4 Mail-Interface

Das *Mail-Interface* übernimmt den Versand aller ausgehenden E-Mails. Zu differenzieren ist hier,

- ob eine E-Mail an die Abuse-Bearbeiter gerichtet ist oder an beliebige andere Empfänger. Im ersten Fall wird überprüft, auf welchen Vorfall sich die E-Mail bezieht, so dass sichergestellt werden kann, dass die E-Mail nur an Abuse-Bearbeiter versandt wird, die auch ausreichende Zugriffsrechte auf die Akte haben.

- wie die E-Mail konkret verschickt werden soll. Üblich ist hier die Verwendung eines SMTP-Servers, auf UNIX-Workstations können aber auch lokal installierte MTAs verwendet werden.

5.5 Maintenance-Tool

Der Abuse-Administrator verwendet das *Maintenance-Tool*, um verschiedenste Wartungstätigkeiten durchzuführen. Periodisch anfallende Aufgaben können dabei als „Cronjobs" auf dem Abuse-Server laufen, zum Beispiel:

- Die Wiederholung des gescheiterten Versands von E-Mails, beispielsweise wenn der SMTP-Server temporär unerreichbar war.

- Die Wiederholung der Aufnahme neu eingegangener E-Mails in die Datenbank, zum Beispiel wenn das Datenbankmanagementsystem nicht erreichbar war.

- Die erneute Ausführung der automatischen Analyse neu eingegangener E-Mails, beispielsweise nach einem Stromausfall beim Abuse-Server.

- Backups der Datenbank und Rollouts.

Interaktiv kann mit dem *Maintenance-Tool* die Benutzerverwaltung und die Aufnahme ausgefilterter E-Mails erfolgen; bei letzteren handelt es sich um E-Mails, die vom Input-Handler nicht direkt in die Datenbank übernommen worden sind. Ziel hierbei ist ein brauchbarer Schutz vor einfachen Denial-of-Service Angriffen auf die Abuse-Bearbeitung. Zum Beispiel können auf diese Weise übergroße E-Mails, die nur darauf ausgelegt sind, das Datenbankmanagementsystem und den *Message-Analyzer* zu überlasten, direkt am Eingang gefiltert und erst nach manueller Inspektion durch einen Administrator ins System übernommen werden.

5.6 Plugin-Server

Der *Plugin-Server* stellt diejenigen Dienste zur Verfügung, die zur Bearbeitung der Abuse-Fälle notwendig sind und entweder besondere Privilegien erfordern oder stark von der lokalen Infrastruktur abhängig sind. Er unterstützt verschlüsselte Datenübertragung und ein einfaches Protokoll zur Authentifizierung der Benutzer und Anforderung der Dienste. Beliebige weitere Dienste können bei Bedarf hinzugefügt werden. Beispiele für bisher vorgesehene Dienste sind:

- Das Ermitteln der für einen Rechner zuständigen Verantwortlichen anhand der IPAdresse.
- Das Durchführen von Portscans zur Diagnose wahrscheinlich kompromittierter lokaler Rechner, über die eine Beschwerde eingegangen ist. Dieses Vorgehen ist durch die lokale Benutzungsordnung gedeckt.
- Das Abklemmen von Rechnern von ihrem Netzzugang durch eine entsprechende Schnittstelle zur Netzadministration.

Um missbräuchliche Anwendung durch die Abuse-Bearbeiter, beispielsweise in Bezug auf die Durchführung von Portscans, erkennen zu können, kann die Benutzung ausgewählter oder aller Dienste automatisch protokolliert werden.

5.7 Die graphische Benutzeroberfläche

Das Client-GUI ist im Wesentlichen ein E-Mail-Client, der auf die speziellen Bedürfnisse der Abuse-Bearbeitung zugeschnitten ist. Im Hauptfenster wird eine Liste der neu eingegangenen Nachrichten und der noch nicht abgeschlossenen Fälle angezeigt, neue Akten können angelegt und Nachrichten zwischen diesen Akten hin- und hergeschoben werden. Besonderheiten hierbei sind:

- Über ein Kontextmenü können beispielsweise nach der Markierung einer IP-Adresse im Text der gerade gelesenen E-Mail verschiedene Aktionen wie Portscans durchgeführt werden, deren Ergebnisse ins Clipboard oder in erstellte E-Mails übernommen werden können.
- Mittels eines ins Abuse-System integrierten „News- und Kommentarsystems" können die Abuse-Bearbeiter zu beliebigen Stichwörtern kurze Artikel verfas-

sen. Die aktuellsten Einträge werden dann in einem News-Fenster angezeigt. Außerdem wird der Text der gerade gelesenen E-Mail nach vorhandenen Stichwörtern durchsucht; gefundene Stichwörter werden explizit aufgelistet. Durch Doppelklicken auf ein solches Stichwort kann der zugehörige Artikel angezeigt werden.

Die über jede Nachricht und jede Akte gespeicherten Meta-Informationen können bei Bedarf verändert werden. So kann beispielsweise der Typ eines Vorfalls manuell angepasst werden, wenn die automatische Analyse keine Resultate geliefert hat, weil entsprechende Stichwörter nicht gefunden worden sind. Die meisten solcher Attribute können ausschließlich aus einer vom Administrator vorgegebenen Liste ausgewählt und nicht frei eingegeben werden – dadurch wird die statistische Auswertung erleichtert; ein und dieselbe Beschwerde könnte sonst von verschiedenen Abuse-Bearbeitern anders klassifiziert werden: „Spam", „UCE (unsolicited commercial email)" und „Werbe-E-Mail" sind hier typische Synonyme.

Das Erstellen ausgehender E-Mails wird insbesondere durch das Textbaustein-System erleichert. Bei den Textbausteinen handelt es sich um häufig verwendete Textpassagen, die auch Variablen und einfache if-Abfragen enthalten dürfen, die vom Abuse-Tool dann durch ihren aktuellen Wert ersetzt bzw. ausgewertet werden. So ist es zum Beispielmöglich, dass jeder Abuse-Bearbeiter in sein Adressbuch einträgt, dass er bestimmte Personen bereits gut kennt; dann können Textbausteine erstellt werden, die dafür sorgen, dass in die Anrede des Empfängers nicht nur der richtige Vor- und Nachname eingesetzt wird (hierfür existiert je eine entsprechende Variable), sondern je nach persönlichem Bekanntschaftsgrad auch ein mehr oder weniger formeller Gruß verwendet wird. Insgesamt stehen mehr als 70 unterschiedliche Variablen für verschiedenste Zwecke zur Verfügung.

Die Textbausteine werden unterschieden durch die Sprache, in der sie geschrieben sind, die Art der E-Mail, für die sie gedacht sind (z.B. Weiterleitungen von Beschwerden), den Abschnitt der E-Mail, für den sie verwendet werden sollen (z.B. Anrede oder Hauptteil) und Stichwörter, für die sie geeignet sind (in der Regel die Art der Vorfallstypen, zu denen sie passen). So kann es beispielsweise beliebig viele englische Textbausteine geben, die für den Hauptteil von Antworten auf Beschwerden über Portscans vorgesehen sind. Die Verwendung der Textbausteine erfolgt dann auf eine der folgenden Arten:

- Die komplette E-Mail wird vom System vorgeschlagen. Dies ist möglich, da das Tool weiß, um welche Art von E-Mail es sich handelt, z.B. um die Antwort auf eine Beschwerde. Die gewünschte Sprache ist im Adressbuch-Eintrag für den Empfänger verzeichnet; das Stichwort, anhand dessen die Textbausteine selektiert werden, entspricht z.B. dem Vorfallstyp „Portscan". Für jeden Abschnitt der E-Mail (z.B. Anrede, Hauptteil, Gruss und Signatur) wird ein Textbaustein ausgewählt. Sollte es mehrere geeignete Textbausteine für diese Kriterien geben, können sie durch die Zuordnung einer Priorität vom System unterschieden werden. Bei mehreren Textbausteinen gleicher Priorität entscheidet die Reihenfolge, in der sie von der Datenbank geliefert werden. Im Idealfall muss der Abuse-Bearbeiter die so vorgeschlagene E-Mail also nur noch per Knopfdruck abschicken.

- Der Bearbeiter kann die Textbausteine für die gesamte E-Mail selbst auswählen. Dazu werden ihm für jeden Abschnitt einer E-Mail alle passenden Textbausteine angezeigt; zu jedem Abschnitt wird jeweils ein Textbaustein ausgewählt und die so erstellte E-Mail kann bei Bedarf noch manuell editiert werden.

- Der Bearbeiter editiert den Text der E-Mail wie bisher manuell und fügt nur bei Bedarf einzelne Textbausteine ein. Dazu werden ihm die vorhandenen Textbausteine anhand der Attribute Sprache, E-Mail-Typ, E-Mail-Abschnitt und Kurzbeschreibung als Baum strukturiert und mit einem kleinen Vorschaufenster angezeigt; der gewünschte Textbaustein kann dann mittels Doppelklicks in die E-Mail übernommen werden.

Für die Verwaltung der Textbausteine, die manuelle Eingabe von Beschwerden ins System, die Suche nach bestimmten E-Mails und Akten sowie statistische Auswertungen existieren entsprechende Dialoge.

6 Prototypische Implementierung

Das vorgestellte Konzept wurde prototypisch in Perl implementiert (17.000 Lines of Code). Die graphische Benutzeroberfläche wurde dabei in Perl/Tk realisiert und ist unter Windows, Linux und diversen UNIX-Derivaten lauffähig.

Die Portierbarkeit des Prototypen auf andere Umgebungen ist derzeit noch dadurch eingeschränkt, dass als *Storage-Mediator* (siehe Abschnitt 5.3) lediglich das Perl Datenbank-Interface (DBI) verwendet wird; entsprechend sind einige der SQL-Anfragen in einem Oracle-spezifischen Dialekt gehalten.

Alle Kernfunktionalitäten wurden vollständig implementiert; der Prototyp ist voll lauffähig und wird derzeit in den Produktionsbetrieb überführt.

Das Abuse-Tool wurde als Open Source Software unter den Auflagen der GNU Public License (GPL) freigegeben und kann auf Anfrage bezogen werden.

7 Zusammenfassung und Ausblick

Die manuelle Bearbeitung von Beschwerden über Abuse-Fälle war bislang eine äußerst zeitaufwendige, aber mangels geeigneter Software unvermeidbare Tätigkeit, die jedoch ein hohes Potential für partielle Automatisierung hat. In diesem Artikel wurde das Konzept eines Softwaresystems vorgestellt, durch das einige Teile des Bearbeitungsprozesses automatisiert und andere Teile wesentlich effizienter als bisher gestaltet werden können.

Eine prototypische Implementierung wird derzeit in den Produktionsbetrieb überführt.

Danksagung:
Die Autoren danken den Mitgliedern des Münchener Netzwerk-Management Teams (MNM Team) für hilfreiche Diskussionen und wertvolle Kommentare zu früheren Versionen dieses Artikels. Das MNM Team ist eine Forschungsgruppe der Münchener Universitäten und des Leibniz-Rechenzentrums der Bayerischen Akademie der Wissenschaften unter der Leitung von Prof. Dr. Heinz-Gerd Hegering.