



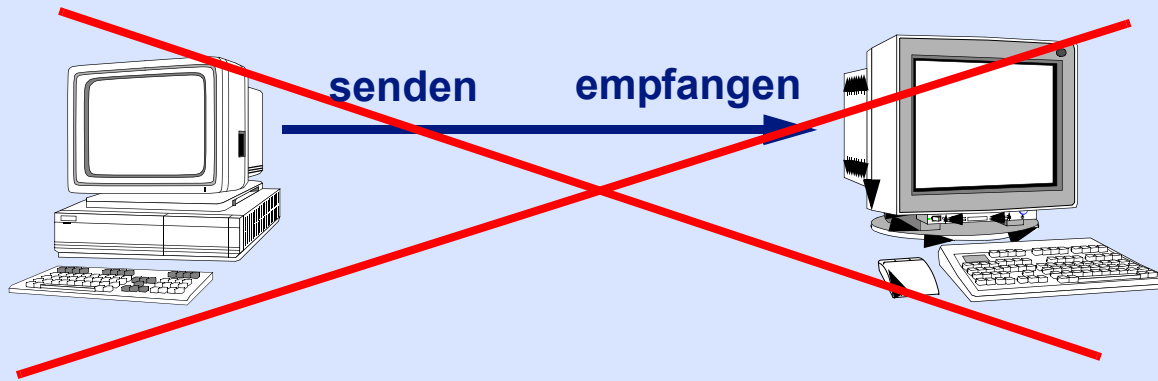
Effizienz und Sicherheit von E-Mail Anwendungen auf PCs

- Status Quo: E-Mail als Problemfall 2
- Übersicht: Wie funktioniert E-Mail 3
- Ein Dienst mit vielen Funktionen... 4
- ...und mit minimaler Sicherheit! 5
- Missbrauch: einige Beispiele 6
- Schutzmaßnahmen am PIK 7
- Klassifizieren: die Guten ins Töpfchen... 8
- Reinigen des Postfachs - MailWasher 9
- Die Hauptfunktionen (I) 10
- Die Hauptfunktionen (II) 11
- MailWasher benutzen 12
- Kurzanleitung 13
- Die Voransicht einer E-Mail 14
- Die Quelltextanzeige einer E-Mail 15

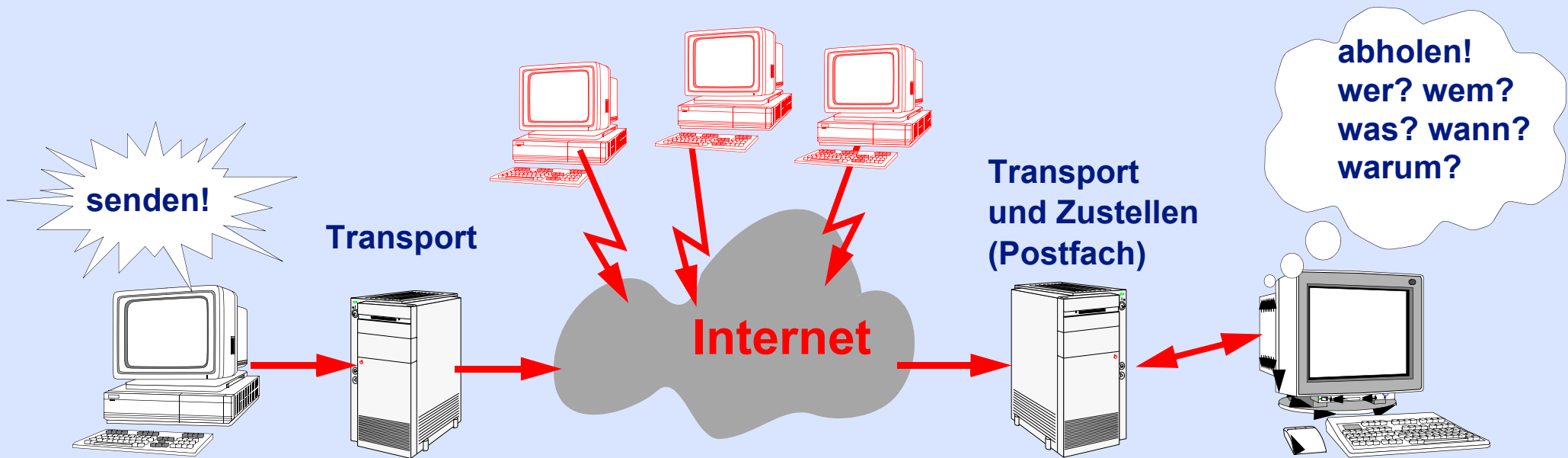
Status Quo: E-Mail als Problemfall

- Spam: das Aussortieren unerwünschter Nachrichten kostet Zeit und Nerven;
Aufwand: bei ca. 5 Min./Tag und 100 Mitarbeiterinnen sind das etwa 8 Std. täglich!
- Viren: im März 2004 wurden ca. 4500 Virenangriffe auf PCs erkannt und abgewehrt - Tendenz steigend;
ein Angriff war erfolgreich, konnte aber auf einen einzelnen PC beschränkt werden;
- Die meisten Angriffe auf PC Endgeräte erfolgen derzeit über E-Mail; im Fall einer Infektion ist allerdings mit einer automatischen und sehr schnellen Ausbreitung im lokalen Netz zu rechnen (Wurm);
- Der Virenschutz erfordert derzeit erheblichen Aufwand.

Übersicht: Wie funktioniert E-Mail



So funktioniert E-Mail nicht:
es gibt keine vertrauenswürdige
Verbindung zwischen Sender
und Empfänger!



Ein Dienst mit vielen Funktionen...

- die Funktionalität von E-Mail Anwendungen wurde in den letzten Jahren stark erweitert:
- Verknüpfung von E-Mail und anderen Anwendungen (z.B. Eudora & Explorer);
- Anhänge der verschiedensten Dateitypen werden automatisch (de)codiert für den Transport über E-Mail (Office Dokumente, Bilder, Archive etc.);
- Integration in das Betriebssystem (Outlook, Internet Explorer) Anhänge werden z.T. automatisch Anwendungen zugeordnet und geöffnet, schlimmstenfalls ausgeführt...
- Grafisch aufbereitete Mails (Bilder, HTML/Web Darstellung), selbst ausführbare Scripte und sog. "Plugins" sind möglich;
- es fehlt ein Sicherheitsmodell zu dieser hohen Funktionalität.

...und mit minimaler Sicherheit!

- neben dem WWW¹ ist E-Mail zum populärsten Dienst des Internet geworden;
- E-Mail ist entstanden als einfacher Dienst zum Austausch von Nachrichten über das Internet;
- die Berechtigung zum Versenden von Mails wird üblicherweise nur über den Zugang zum Netzwerk geprüft;
- eine Verifikation der Absenderangabe findet nicht statt;
- nur beim Abholen von Mails zum Endgerät findet eine Authentifikation über Login-Name und Passwort statt;
- die Daten werden unverschlüsselt im Internet übertragen (Vergleich: Postkarte - kann jeder lesen);
- Fälschungen sind sehr leicht anzufertigen.

1. World Wide Web

Missbrauch: einige Beispiele

- Nachladen von Bildern bewirkt unerwünschte Webzugriffe; durch Zusenden entsprechender Mails wird ein PC auf eine unerwünschte Webseite “entführt”; dort werden z.B. Daten eingesammelt oder Angriffe ausgeführt;
- Verknüpfung von Programmen vergrößert die Angriffsfläche: wenn eine E-Mail Anwendung den Internet Explorer zur Ansicht verwendet, kann der Rechner über dessen Sicherheitslücken angegriffen werden;
- Verwendung von Adresslisten aus dem Internet für gezielte Virenangriffe (deswegen wurden die E-Mail Adressen aus der Staff-Liste des PIK entfernt!);
- Gefälschte Absender verleiten zum Öffnen von Anhängen.



Schutzmaßnahmen am PIK

- der Mail-Transportdienst nimmt eine formale Prüfung vor und weist bekannte “Spam- und Virenschleudern” ab; diese Maßnahme wirkt VOR dem “Einwurf” in das Postfach des Anwenders;
- Problem: ständig wechselnde Absender machen die Erkennung schwer; es könnten auch relevante Mails abgewiesen werden;
- PC: Antivirus-Software / ausfiltern bekannter schädlicher Anhänge, scannen mit verschiedenen Methoden passiert NACH dem “Abholen” zum Endgerät;
- Problem: Viren haben den PC bereits erreicht - dies ist also die letzte mögliche Schutzmaßnahme - kurz vor dem Notfall...
- Frage: Warum sollte man überhaupt etwas abholen, das schon bei der einfachen Ansicht als Müll erkannt werden kann?

Klassifizieren: die Guten ins Töpfchen...

- Aufgabe: nur erwünschte Mails abholen;
- Spam automatisch erkennen:
viele Spamverteiler sind bekannt und in sogenannten RBLs¹ eingetragen;
- Viren automatisch erkennen:
viele Viren sind einfach am Dateityp des Anhangs erkennbar, ohne daß ein exakter Vergleich vorgenommen werden muß;
- Kontrolle bleibt bei den Anwendern:
die Aufteilung in “erwünscht/unerwünscht” wird zwar automatisch vorgenommen, aber die Empfänger können korrigierend eingreifen - sie treffen selbst die Entscheidung.

1. Remote Black List

Reinigen des Postfachs - MailWasher

- in den Postfächern werden E-Mails solange angesammelt, bis sie abgeholt und dabei gelöscht werden; eine Kopie liegt dann im Mail-Ordner der Anwenderin;
- MailWasher ist ein Windows-Programm, mit dem Postfächer beobachtet und bearbeitet (Löschaufträge!) werden können, ohne daß die Inhalte zum Endgerät übertragen werden;
- MailWasher überträgt nur die “Kopfzeilen” (ähnlich den Angaben auf einem Briefumschlag) und klassifiziert die Nachrichten: Spam, Virus, Normal und einige mehr...
- aufgrund der Klassifikation schlägt MailWasher vor, welche Mails im Postfach zu löschen sind;
- die Anwenderin überprüft - ggf. korrigiert - diese Vorschläge und wendet sie dann auf das Postfach an.



Die Hauptfunktionen (I)

- MailWasher ist sehr einfach zu benutzen, mit wenigen Befehlen und intuitiver Bedienung;
- das Programm dient nur zur Vorverarbeitung, nicht als Ersatz für eine Mail-Anwendung;
- MailWasher arbeitet neben der üblichen Mail-Anwendung und stört diese nicht;
- das Postfach wird regelmäßig abgefragt und “Umschlagdaten” werden, zusammen mit der automatischen Klassifikation, angezeigt;
- zwei externe “Blacklists” werden zur Erkennung von Spam abgefragt, außerdem verwendet MailWasher heuristische Methoden¹ zur Erkennung von Spam.

1. Merkmalsanalyse - z.B. Anhänge, bei denen versucht wird, den ausführbaren Charakter zu verdecken

Die Hauptfunktionen (II)

- Viren werden aufgrund einer heuristischen Analyse und durch Vergleich mit bekannten Mustern markiert;
- MailWasher ist kein Ersatz für einen aktuellen Virens Scanner!
Viren und Würmer haben neben E-Mail noch weitere Ausbreitungsmethoden; außerdem ist Heuristik nur eine Ergänzung zu bewährten Signaturverfahren - NVC ist in diesem Bereich viel stärker;
- bei Verwendung von MailWasher wird die Netzlast geringer, denn nur relevante Mails werden übertragen (große Anhänge, doppelt verschickte Mails etc. werden schon im Postfach gelöscht);
- ein Löschauftrag in MailWasher ist *endgültig!*

MailWasher benutzen

- das Programm wird auf ausgewählten PCs von D&C installiert
- weitere Infos: <http://ce:7000/dc-it/howto/mailwasher>

The screenshot shows the MailWasher version 2.0 interface. The title bar reads "MailWasher version 2.0". The menu bar includes "File", "Email", "Tools", and "Help". The toolbar contains icons for "Check Mail", "Stop", "Process Mail", and "Mail Program". A "Tell a Friend" button is also visible. The main area displays a list of emails with the following columns: Delete, Bounce, Blacklist, Status, Size, From, Subject, Sent, and To. The status column contains various entries such as "Origin blacklisted by SpamCop", "PIK Broadcast", "Blacklisted", and "Possible Virus". The status bar at the bottom indicates "Mail was last checked 1 minute ago".

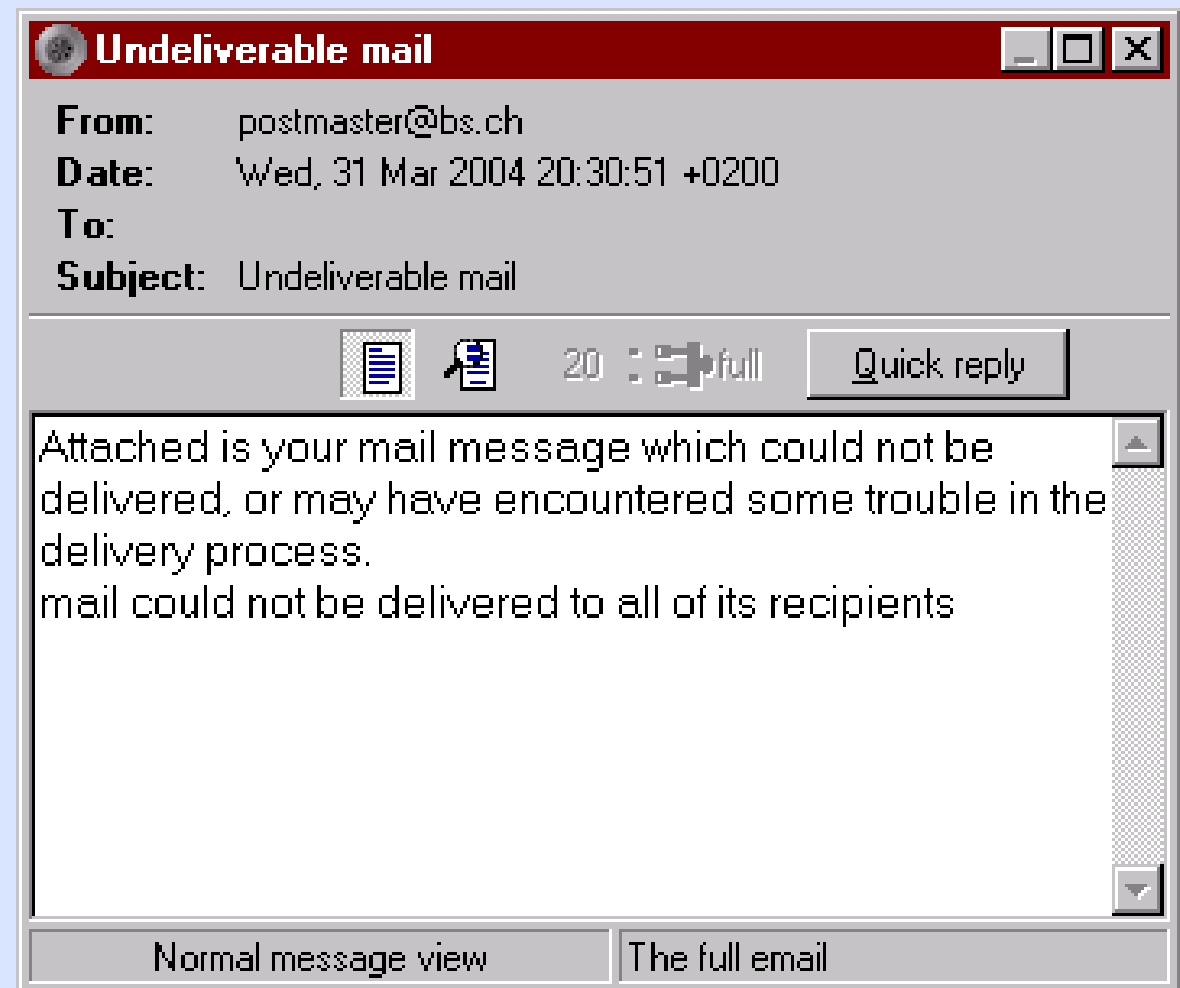
Delete	Bounce	Blacklist	Status	Size	From	Subject	Sent	To
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Origin blacklisted by SpamCop	3,9KB	Reba Reyna (np02	RE:splice Hello ! zzmmkqjs	9 Sep 2003, 10:39am	gerhard@pik-potsdam.de
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Origin blacklisted by SpamCop	4,2KB	mjckmbinvestpickst	Breaking News CFCU make million dollar advanceme	9 Sep 2003, 6:03am	gibietz@pik-potsdam.de
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Origin blacklisted by SpamCop	2,5KB	shuawei@tom.com	gibietz	9 Sep 2003, 11:09am	gibietz@pik-potsdam.de
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Origin blacklisted by SpamCop	2,1KB	Santos Fuller (w06y	ially comson epejtsf pkt	"Tue, 09 Sep 03 05:3l	webmaster@pik-potsdam
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	PIK Broadcast	5,4KB	Detlef Sprinz (dsprir	Lomborg on recent weather extremes	8 Sep 2003, 11:10pm	pik.all
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Blacklisted	1KB	bs020@2to2.net	☘ÄËËÄ:0-ijxÖÄ_ß	8 Sep 2003, 8:45pm	gibietz@pik-potsdam.de
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Blacklisted	7,8KB	Landscapes painter	[ADV] LE LORRAIN Claude Gellee	9 Sep 2003, 1:08am	webmaster@pik-potsdam
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Possible Virus	100,2KB	krings@fh-bingen.d	Thank you!	8 Sep 2003, 7:50pm	webmaster@pik-potsdam
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Possible Virus	98,3KB	schakki87@web.de	Thank you!	8 Sep 2003, 7:53pm	webmaster@pik-potsdam
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Possible Virus	99,3KB	sony666@users.so	Re: Wicked screensaver	8 Sep 2003, 7:59pm	webmaster@pik-potsdam
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Possible Virus	101,4KB	asre@uiuc.edu	Re: Approved	8 Sep 2003, 8:04pm	webmaster@pik-potsdam
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Possible Virus	102,0KB	ken.tanaka@noaa.	Re: Details	9 Sep 2003, 2:27am	webmaster@pik-potsdam
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Possible Virus	102,5KB	a1-web@gr.cs.utah	Your details	9 Sep 2003, 2:40am	webmaster@pik-potsdam
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Possible Virus	97,8KB	netfwsdk@microsoft	Re: That movie	9 Sep 2003, 2:48am	webmaster@pik-potsdam
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Possible Virus	99,8KB	line@microsoft.hr	Re: Approved	9 Sep 2003, 3:07am	webmaster@pik-potsdam
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Possible Virus	102,4KB	cindywye@hotmail.	Re: Your application	8 Sep 2003, 11:27pm	webmaster@pik-potsdam

Kurzanleitung

- sortieren nach einem Feld: in den Spaltenkopf klicken
- auf “Freunde”-Liste (Friends) setzen: Taste [+]
Mail bleibt im Postfach bis zum Abholen;
- auf “Blockade”-Liste (Blacklist) setzen: Taste [-]
diese Mail und alle zukünftigen Mails dieses Absenders werden zum Löschen markiert;
- Nur zum Löschen markieren: [D] oder Klick in’s “Delete”-Feld;
- Aktion ausführen (löschen!): Schalter “Process Mail” klicken;
- vor dem Ausführen (löschen!) immer die Liste der zu löschenden Mails kurz durchsehen!
- dazu sortiert man die Liste am besten nach dem “Delete”-Feld;
- Virus Mails sollte man nie auf die “Blacklist” setzen, da die Absenderangabe meistens gefälscht ist.

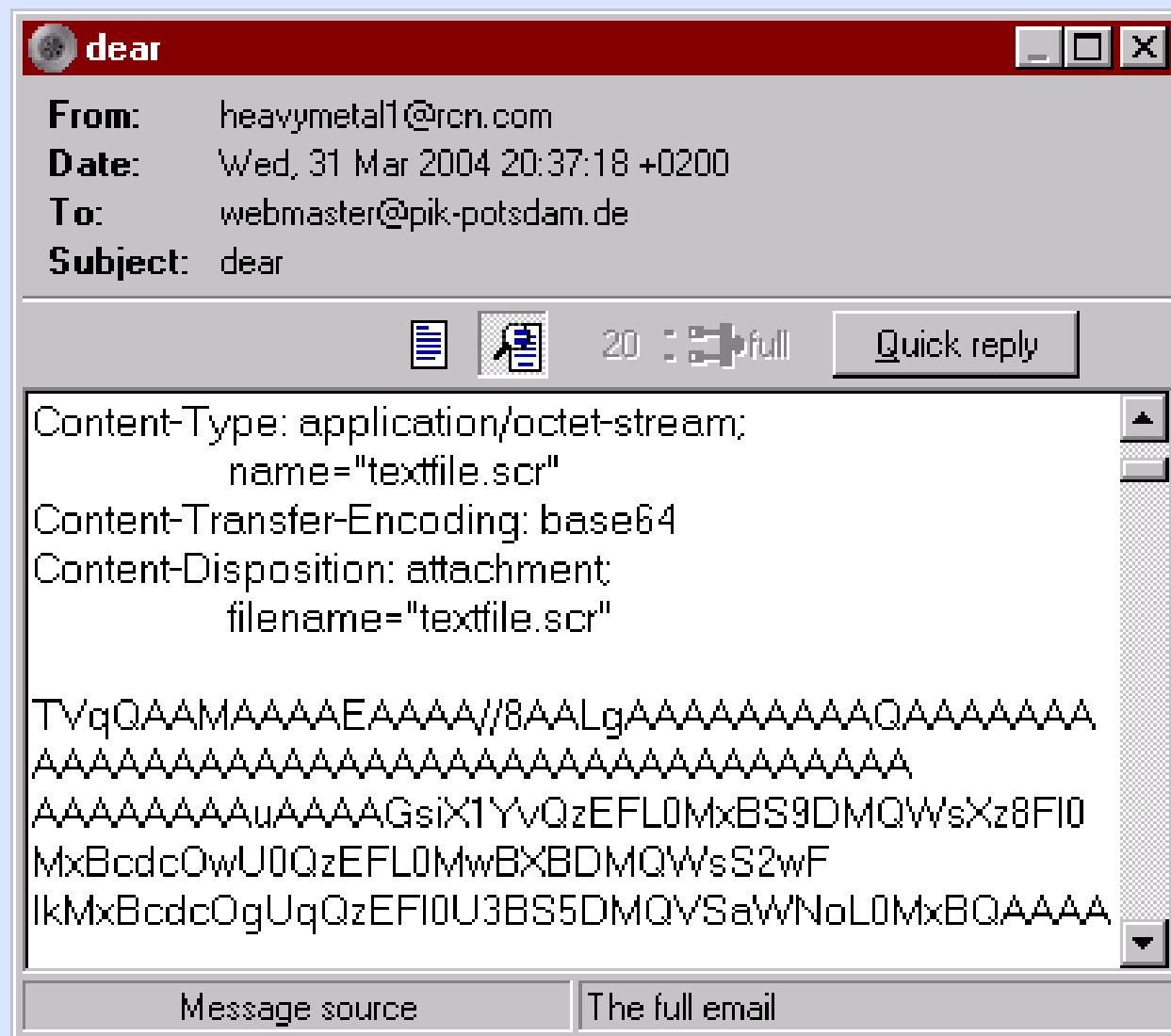
Die Voransicht einer E-Mail

- wird durch Doppelklick auf eine Mail geöffnet (alternativ: Eingabe- oder Leertaste);
- zeigt nur den als Text darstellbaren Inhalt;
- vermerkt bei HTML Mails, wohin ein Link wirklich zeigt - wichtig!
- ist eine sichere Ansicht (keine Virusgefahr);
- Abb.: Text-Teil einer Virus-Mail.



Die Quelltextanzeige einer E-Mail

- wird aus der Voransicht aufgerufen;
- Anhänge werden erkennbar;
- Viren werden erkennbar;
- alle Versanddaten (“Briefumschlag”) werden gezeigt;
- sieht wild aus, kann aber sehr nützlich sein;
- Abb.: Quelltext einer Virus-Mail.



Danke für Ihre Aufmerksamkeit!

- Wie geht's weiter?
- kurze Vorführung
wie im richtigen Leben :-)
- MailWasher im Alltag einsetzen;
- die Friends- und Blacklist trainieren;
- Sicherer arbeiten und freuen darüber, wie schnell der Müll weggespült wird.