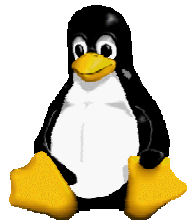
About HagK

- HagK ~ Hagen Kühnel
- Aufgabengebiet:
  - ➔ Systemadministration
  - ➔ Systemkonzeption & -analyse
  - ➔ www-Anbindungen, www-Applikationen

  - Status: Freiberufler

www.hagk.de hagk@hagk.de

http://www.hagk.de/bwn/



E-Mail ~ Kenndaten

- historisch: als Killermedium bezeichnet
- Mehr als 20 Millarden e-Mails täglich weltweit.
- Hauptverbreitung für Viren und Dialer
- Schnelle Übermittlung von Informationen und Schriftstücken, aber auch versehentlich
- Fälschungen sehr leicht möglich

e-Mail ~ Protokolle und Dienste

- * Simple Mail Transfer Protocol (SMTP)

Zum Versand und Transport einer e-Mail. RFC-819, RFC-821, RFC-822

- * Post Office Protocol * (POP3, APOP)

Zum Abrufen der eingegangenen Mails. Die Mail kann nach dem Abruf auf dem Server verbleiben oder gelöscht werden. RFC-1939 und RFC-2449

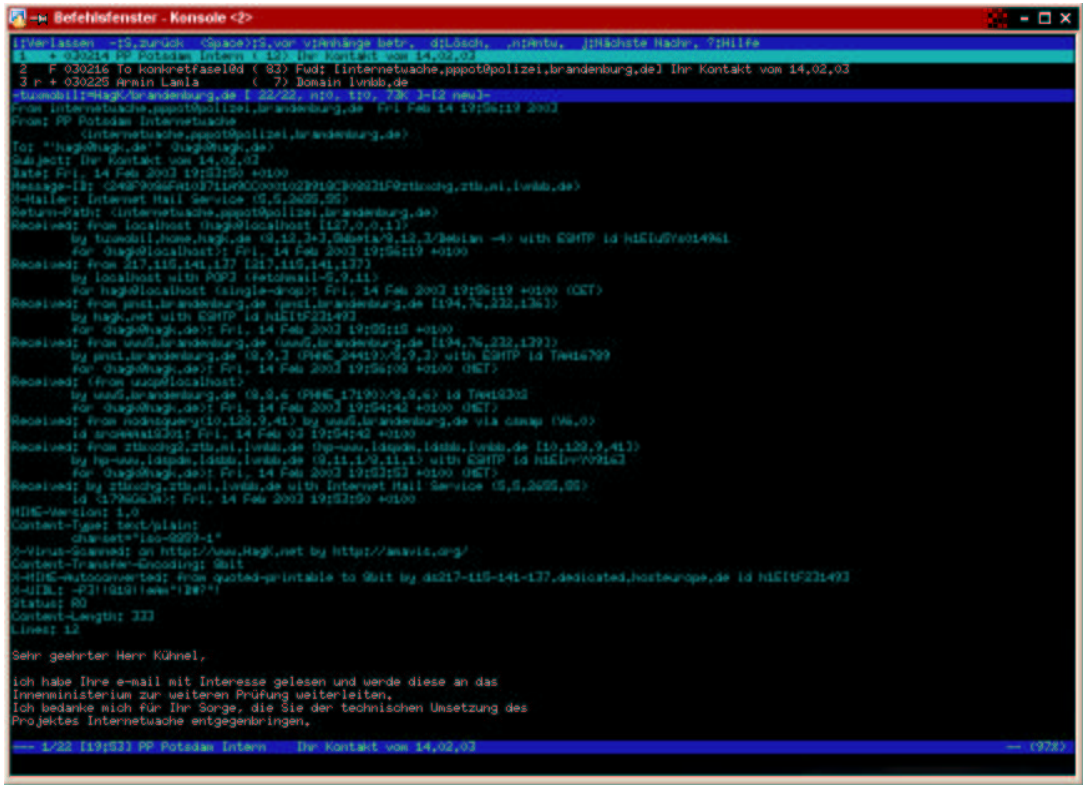
- Internet Message Access Protocol (IMAP)

Zum Bearbeiten der eingegangenen Mails als Ergänzung oder Alternative zu POP. Die Bearbeitung erfolgt auf dem Mailserver (remote access). RFC-2060

Standardprotokolle: unverschlüsselte Datenübertragung!

e-Mail Bestandteile

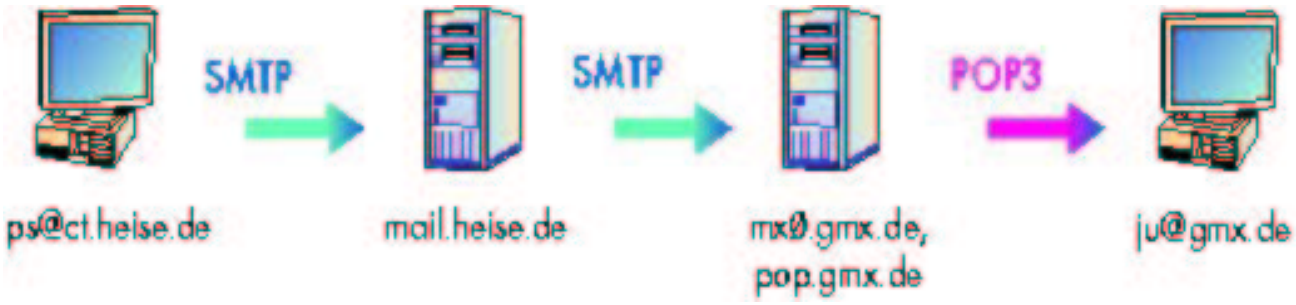
- Netzstruktur-informationen
  (welche Rechner waren am Transport beteiligt)
- Benutzte Software
  (veraltet mit Sicherheits-lücken --> angreifbar?)
- Nutzdaten
  (auch Viren, SPAM etc.)



e-Mail Wege (1)

Direktzugang / Standleitung

- Der Sender übergibt die Mail seinem Provider, der sie an den Provider des Empfängers weiterleitet.
- Der Empfänger liest die Mail dort (IMAP) oder holt sie dort ab (POP3).



Bildquelle: c't 20/2002 S. 122

Heise Verlag, Hannover

e-Mail Wege (2)

LAN/ lokales Netzwerk

- Der Sender übergibt die Mail dem lokalen Mailserver, der sie an einen internen user oder an einen externen Server weiterleitet.

Bildquelle: c't 20/2002 S. 122

Heise Verlag, Hannover

Verfügbarkeit Mailservice (1)

- e-Mail ist kein Echtzeitmedium
- Warnung des Absenders nach 4 Stunden und 5 Tagen bei Nichterreichbarkeit (Standard)
- Redundanz durch mehrere zuständige Mail eXchange Server des Empfängers (kann)
- Information des theoretischen Absenders (FROM) bei Empfangsverweigerung durch die Mailverteilung des Empfängers (Problem 'geborgte Absenderadressen' für Spam)
- Derzeit: wo eine Mail 'hängt' (oder gelöscht wurde) ist unbekannt, bis zu Ihrer Rückmeldung ~ eine Lesebestätigung ist freiwillig
- IETF-Entwürfe für ein Message Tracking Protocol (msgtrk)

Verfügbarkeit Mailservice (2)

- Shared Mailserver (die auch andere Dienste bedienen) stoppen unter hoher Last den Mailservice
- TCP-IP basierte Netzwerke haben keine Prioritätsstufen
- Quality of Service (QoS) erst am Anfang der Umsetzung, jedes Glied der Kette (inbesondere Router) müssen QoS unterstützen
- Weltweite Abrechnung der QoS unklar, netzinterne Lösungen vorhanden (Bsp: Strato-SkyDSL Bandbreitengarantie)
- Server-downtime je nach Service Level Agreement (SLA) des Providers, 99,9% Verfügbarkeit sind 8 Stunden offline

Zeitaufwand der Kommunikation

- Sichtung eingehender Email (Interpretation)
- Aussonderung von fehlgeleiteter Email und SPAM (Filterung)
- Weiterleitung an Empfänger/ Bearbeiter (Selektion und Routing)
- Priorisierung von Email zur Weiterverarbeitung (Klassifikation)
- Aufbereitung von Email zur Weiterverarbeitung z.B. Adressaufnahme oder Bestellaufnahmen (Extraktion)
- Beantwortung (Zuordnung einer vorbereiteten Standardantwort)
- Archivierung und Verschlagwortung, Indizierung

kommeriell: www.tonxx.com 'Responsio' z.B. als Outlook-Plugin

Beispiel-Zeitaufwand: zwischen 0,5 s (gefilterter SPAM) bis 30 min (fachliche Antwort) pro e-Mail, abhängig auch vom Handling des e-Mail-Programmes

OpenSource Projekte

- Mailserver (MTA) wie Sendmail, Postfix und Exim sind frei verfügbar und repräsentieren den Standard. Bei der Kommunikation mit Unbekannten ist der kleinste gemeinsame Nenner zu wählen (der Standard). Standards werden von der IETF in RFCs niedergeschrieben.
- SPAM-Filterung wird im unixoiden Umfeld meist mit SpamAssassin realisiert. Die Erkennungsrate liegt unkonfiguriert bei 80%, die Konfiguration und Anpasung ist schwierig und zeitaufwendig. Die Nutzung bedarf hoher Ressourcen auf dem, mit der Filterung beauftragten Server.
- Archivierung und Workflow mit OTRS (webbasiert)
  - Schwierige Installation, auch auf SuSE-Systemen
  - Längere Bearbeitungszeiten, da mausbasierte Bedienung
  - Schwerpunktbereich Supportanfragen

[OTRS] Hagen Kühnel (hagk@hagk.de) Don 19 Jun 13:25:59 2003

Abmelden | Queue-Ansicht | Telefon-Ansicht | Werkzeuge | Einstellungen | Statistik | Neue Nachrichten (0) | Eigene Tickets (0)

[Inhalt Ticket#: 2003051527000265] [Alter: 34 Tage 23 Stunden]

Sperren - Priorität - Historie - Besitzer - Notiz - Kunde - Freie Felder - Drucken - Warten - Schließen

Erstellt: 2003-05-15 14:23:42

|-->>>**Kunde (E-Mail an extern) (klar) 2003-05-15 14:23:42**
|-->Agent (Notiz für intern) 2003-05-15 14:43:12
|-->Agent (Notiz für intern) 2003-05-15 14:57:50

Von: Hagen Kühnel - HagK <hagk@hagk.de>
An: otrs@hagk.net
Betreff: no answer

```
--
52/ 70
>>> darf man die relevanten punkte nicht zitieren
>>> nur weil es aus der new-york-times stammt?
>> Ich möchte künftig noch in die USA ein- und wieder ausreisen können.
> Wieso eigentlich?
Weil man da nicht bleiben will?
        Sebastian Posner in <am5h1s$2ufdp$10@ID-45817.news.dfncis.de>
```

Status: erfolgreich ges[...]
Priorität: 3 normal
Queue: Misc::ToBuS
Sperren: frei
Kunden#: hagk@hagk.de
Zugewiesene Zeit: 0
Eskalation in: -33 Tage 23 Stunden
Besitzer: hagk

Kunden-Info: keine

Antwort erstellen (E-Mail):

- empty answer

Kunden kontaktieren (Telefon):

- Anrufen

Artikel

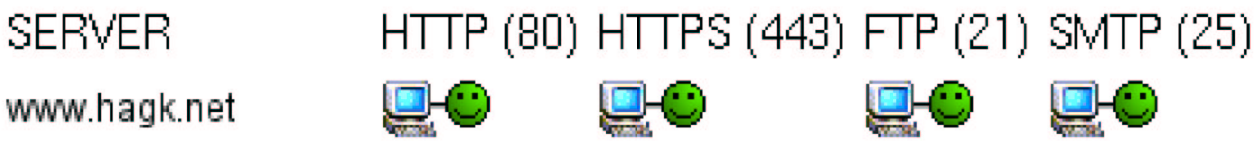
Weiterleiten Bounce Teilen

Wechsele Queue:

ToBuS | Verschieben

Verfügbarkeit & Redundanz

Die Verfügbarkeit der Mailserver hängt vom DomainNameService und den Mailserver(n) ab. Zur Überwachung der Server können kleine Skripte beitragen, die die tatsächliche Erreichbarkeit überprüfen. Im Fehlerfall können Routinen anlaufen, die den festgestellten Fehler auf Gültigkeit überprüfen und Messaging-Regeln in Gang setzen (SMS, Cityruf, eMail, Telefonanruf). Redundante Mailserver sollten grundsätzlich in einem seperaten Netz stehen, damit bei Nichterreichbarkeit von Mailserver1 durch z.B. Routing-Probleme des Providers, auf Mailserver2 ausgewichen werden kann. Die beste Netzstruktur haben Sie genau dann, wenn Sie überhaupt nicht bemerken, dass gerade ein riesiges Problem besteht.

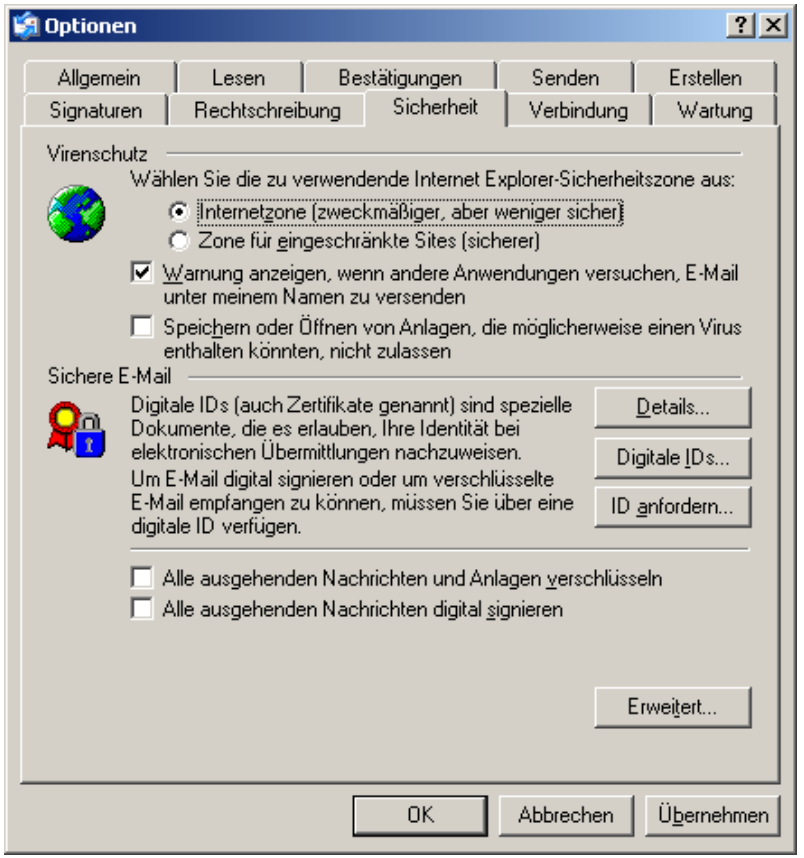


Am Rande ~ Outlook, das trojanische Pferd?!

Probleme durch die Verknüpfung der Sicherheitseinstellungen mit dem Betriebssystem und damit sämtlichen Internetanwendungen und mangelhafter default-Einstellungen.

Daher: Nutzung der 'eingeschränkten Zone' (der Internetoptionen) und resolute Einschränkungen der aktiven Komponenten nötig.

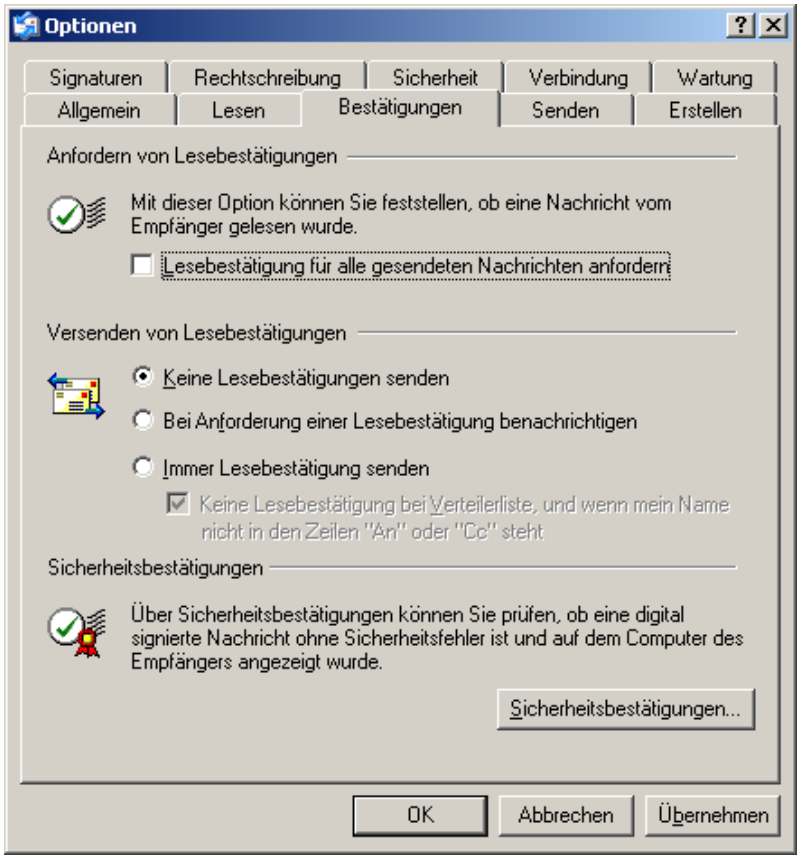
HTML-Vorschau ist nicht abschaltbar, daher ist eine Verifizierung der e-Mail-Adresse durch Counter-Pixel möglich.



Am Rande ~ Outlook, das trojanische Pferd?!

Lesebestätigungen, falls der Absender davon ausgeht, dass Sie nur einmal jährlich in Ihr Postfach gucken.

Interessante Profile lassen sich über die Gewohnheiten des e-Mail-Abrufs ebenfalls erstellen und der Empfänger weiß, dass Sie sich mit einer Antwort über zwei Stunden Zeit gelassen haben und ihn also nicht bevorzugt und schnell behandelt haben.



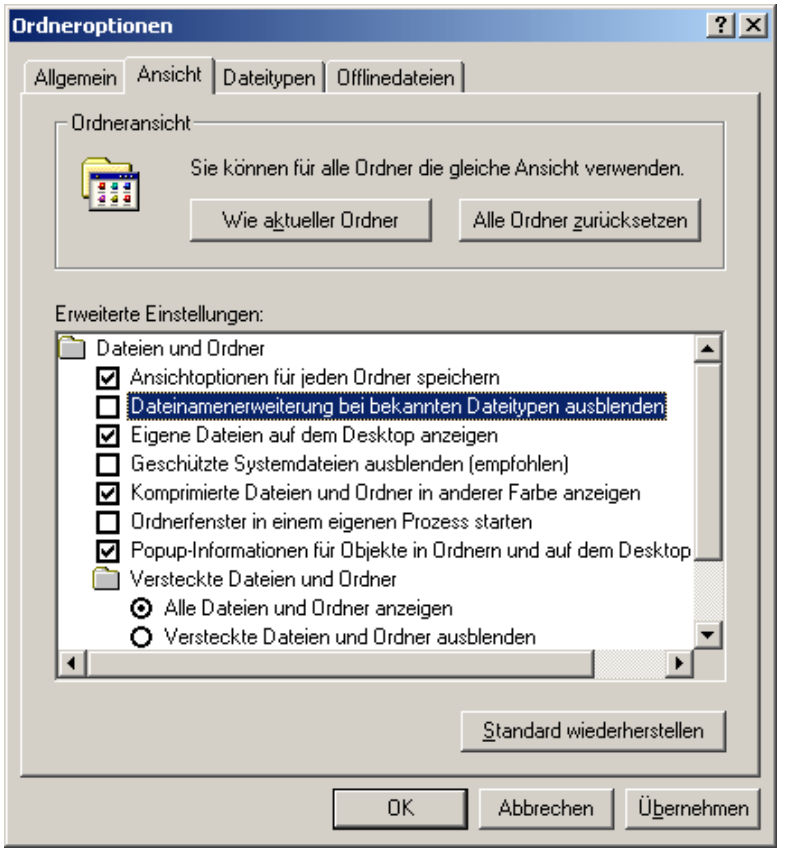
Am Rande ~ Outlook, das trojanische Pferd?!

Dateinamen und ihre Erweiterungen sind für DOS und damit auch Windows (NT) überlebenswichtig.

Ein_Bildschirmschoner.scr[.exe] kann auch ein Virus oder Dialer sein.

Im Auslieferungszustand werden bekannte Dateiendungen ausgeblendet. Da .scr eingeblendet wird hier wohl also noch etwas bekanntes dranhängen.

Dieses Verhalten ist in den Einstellungen des Windows-Explorers änderbar.



Am Rande ~ Outlook, das trojanische Pferd?!

Outlook kann filtern.
[Menü Nachricht->Regel für Nachricht]

Durch solche Filterregeln kann die Auswertung von, als SPAM identifizierten oder verdächtigen Mails in bestimmte Ordner erfolgen. Ebenso können Mails mit Dateianhängen und/oder bestimmten Betreffs 'wegsortiert' oder gelöscht werden.