SPAM und AVG §13: Wie geht man damit um?

Peter Pfläging
Stadt Wien
MA 14 - Rechenzentrum
Leiter Stabstelle
Koordination
<pfp@adv.magwien.gv.at>

© 2007 Stadt Wien - Peter Pfläging <pfp@adv.magwien.gv.at>

Agenda

- Wo ist das Problem?
- SPAM und seine Verhinderung
- Technische Massnahmen
- Lösungsansatz im rechtlich / organisatorichen Bereich
- Fragen?

© 2007 Stadt Wien - Peter Pfläging <pfp@adv.magwien.gv.at>

Wo ist das Problem?

- SPAM (unerwünschte Werbung) wird immer stärker!
  - für die Stadt Wien ca. 35% des einkommenden Mailverkehrs
- Technische Methoden zur Blockierung nicht immer effektiv.
  - zu scharf: falsch markierte SPAM (False positives)
  - zu schwach: keine Unterstützung der Anwender

- AVG §13: Einbringen der Bürger mit allen möglichen Methoden
  - das heißt auch: e-Mail
  - Markierung von e-Mail Einbringen als SPAM problematisch
  - vom Mailserver angenommen => eingebracht von der Partei

© 2007 Stadt Wien - Peter Pfläging <pfp@adv.magwien.gv.at>

IN ZUKUNFT WIEN :Planen. Gestalten. Handeln.
StaDt Wien Wien ist anders.

SPAM und seine Verhinderung

- Zwei prinzipielle Methoden:
  - Erkennung auf Basis von Blacklists
    - Anhand von Absendern
    - Charakterisken der e-Mail
    - Mailserver von SPAMmern oder offene Relays
  - Erkennung auf Inhaltsbasis
    - Bayesianische (lernende) Filter
    - Filter auf Basis von Charakteristika des Inhalts

- Zeitpunkt der Erkennung:
  - Während der Übertragung im SMTP Protokoll
  - Auf dem Mailserver der Organisation

- **Übrigens gelten die selben Regeln auch für Viren!**

© 2007 Stadt Wien - Peter Pfläging <pfp@adv.magwien.gv.at>

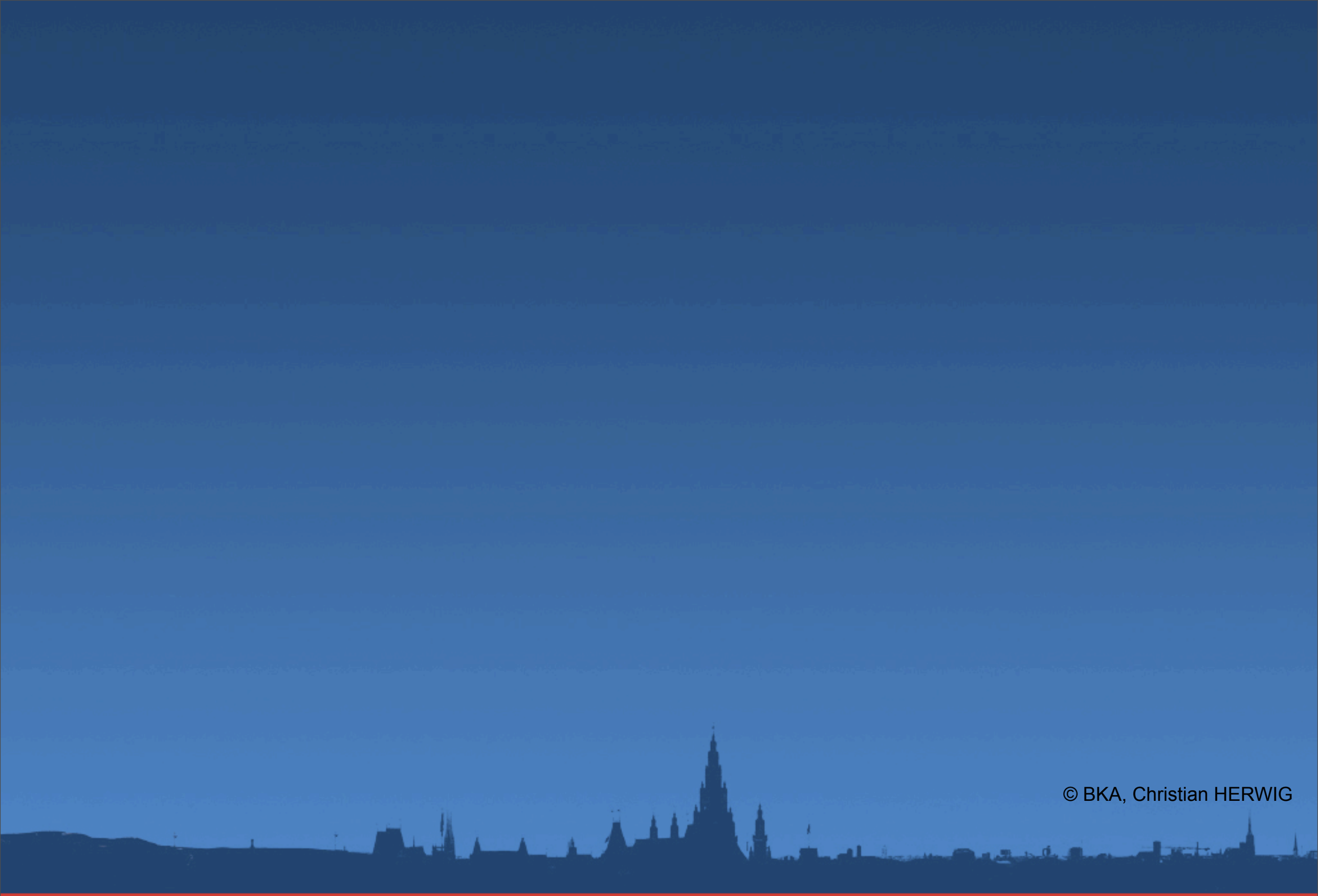
IN ZUKUNFT :WIEN :Planen. Gestalten. Handeln.
StaDt Wien Wien ist anders.

Technische Massnahmen

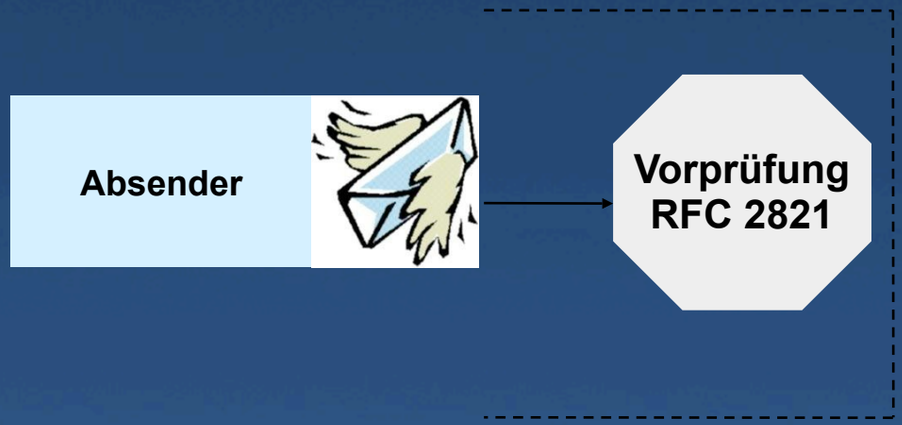
- Virenscan und SPAM Erkennung möglichst weit vorn im Mailserver
- Mailserver, welche Blacklisting und Greylisting unterstützen

- Schadhafte Mails, die nicht weit vorn erkannt werden nur reinigen und markieren, nicht wegwerfen
- Benutzer mit Schulung und Tools unterstützen

© 2007 Stadt Wien - Peter Pfläging <pfp@adv.magwien.gv.at>

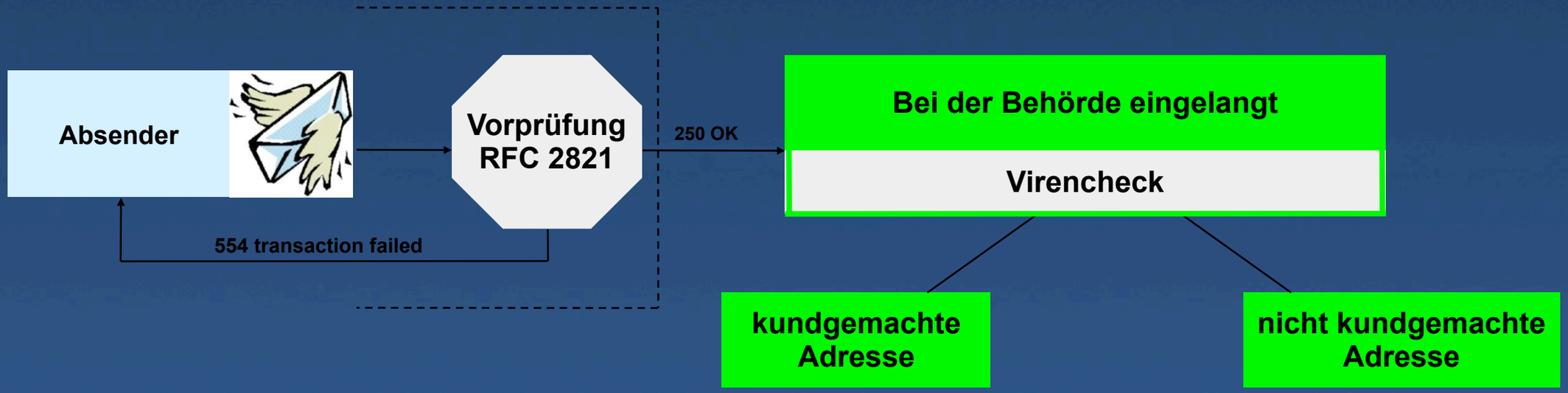


© 2007 Stadt Wien - Peter Pfläging <pfp@adv.magwien.gv.at>



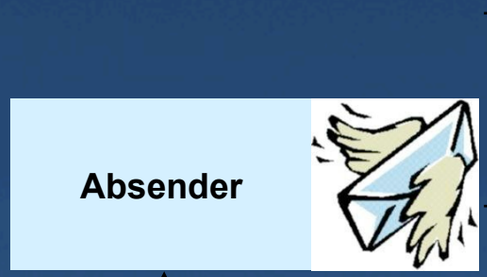
© BKA, Christian HERWIG

© 2007 Stadt Wien - Peter Pfläging <pfp@adv.magwien.gv.at>



© BKA, Christian HERWIG

© 2007 Stadt Wien - Peter Pfläging <pfp@adv.magwien.gv.at>



Anbringen erkennbar

© BKA, Christian HERWIG

© 2007 Stadt Wien - Peter Pfläging <pfp@adv.magwien.gv.at>

Absender

Vorprüfung RFC 2821

250 OK

554 transaction failed

Bei der Behörde eingelangt

Virencheck

kundgemachte Adresse

Weiterleitung

nicht kundgemachte Adresse

Ja

Bearbeitung

Bearbeitung

Ja

Anbringen erkennbar

Nein

keine weitere Bearbeitung z.B. bei SPAM

Anbringen unvollständig

© BKA, Christian HERWIG

© 2007 Stadt Wien - Peter Pfläging <pfp@adv.magwien.gv.at>

IN ZUKUNFT WIEN :Planen. Gestalten. Handeln.

StaDt Wien Wien ist anders.

Absender

Vorprüfung RFC 2821

250 OK

554 transaction failed

Bei der Behörde eingelangt

Virencheck

kundgemachte Adresse

Weiterleitung

nicht kundgemachte Adresse

Ja

Bearbeitung

Bearbeitung

Ja

Anbringen erkennbar

Nein

keine weitere Bearbeitung z.B. bei SPAM

Verbesserungsauftrag

Ja

Anbringen unvollständig

Nein

Erledigung

© BKA, Christian HERWIG

© 2007 Stadt Wien - Peter Pfläging <pfp@adv.magwien.gv.at>

IN ZUKUNFT WIEN Planen. Gestalten. Handeln.

StaDt Wien Wien ist anders.

Lösungsansätze im rechtlich / organisatorischen Bereich

- Differenzierung von persönlichen und „kundgemachten“ Adressen
- Kennzeichnung von „verdächtigen“ e-Mails
- Vermehrte Bereitstellung von Webformularen als Kommunikationsmittel
- Schulung der Anwender

- e-Mail untersagen ist nicht die Lösung:
  - im Internet ist e-Mail immer noch die Kommunikationslösung Nr. 1

- Pragmatischer Umgang mit dem Medium
  - Parallelen zu Briefpost
- Dokumentation der Vorgangsweise (Logfiles, ELAK, ...)

© 2007 Stadt Wien - Peter Pfläging <pfp@adv.magwien.gv.at>

Fragen?

- Dokumente der Arbeitsgruppe Q-SI (http://reference.e-government.gv.at)
- RFC 2821 (http://www.ietf.org/rfc/rfc2821.txt)
- Realtime Blackhole Lists (http://de.wikipedia.org/wiki/Realtime_Blackhole_List)
- Greylisting (http://de.wikipedia.org/wiki/Realtime_Blackhole_List)

Vielen Dank

-peter pfläging

© 2007 Stadt Wien - Peter Pfläging <pfp@adv.magwien.gv.at>