

# Spam-Mail Behandlung

## Arbeitspapier des Arbeitskreises „Die zukünftige Entwicklung des BDSG in Deutschland“

Version: 27.09.2004

Die Handhabung von Spam-Mails stellt in den Unternehmen der Privatwirtschaft und auch in den Bereichen der öffentlichen Stellen ein zunehmendes Problem dar. Um Denkanstöße zu unterbreiten wurde zunächst eine **Sammlung der Probleme** vorgenommen.

1. Beim Ausfiltern von Spam-Mails kann es zu sogenannten „false positives“ (fehlerhaft als Spam Mails interpretierte echte Mails) oder „false negatives“ (nicht erkannte Spam-Mails) kommen.
2. Die Information der adressierten Mitarbeiter über eingegangene Spam-Mails ist auch in Zeiten von Urlaub und Krankheit zu gewährleisten, da false positives erkannt und bearbeitet werden müssen.
3. Die Frage ist zu klären, inwieweit der Arbeitgeber als Spam erkannte Mails direkt löschen darf oder ob die Mails in einen Quarantäne-Ordner abgelegt werden müssen (siehe Punkt 1)
4. Eine korrekte Datenschutzregelung ist zu treffen, entweder über eine Vereinbarung mit der Arbeitnehmervertretung oder die Zustimmung der Mitarbeiter ist einzuholen.
5. Es ist zu klären, wie technisch gesehen die Filterung praktiziert wird, d.h. inwieweit Einfluss genommen werden kann auf die Erkennungsmechanismen.
6. Durch entsprechende betriebliche Regelungen ist zu gewährleisten, dass es nicht zu Verletzungen des Brief- und Fernmeldegeheimnisses kommt.
7. Die Dauer der Aufbewahrung von in Quarantäneordnern abgelegten Mails ist zu klären.
8. Die Auswirkungen von der Nichtbeachtung/Nichterkenntnis von false positives ist zu bewerten und durch entsprechende Gegenmaßnahmen sicherzustellen, dass keine rechtsverbindlichen Informationen unbeachtet bleiben.
9. Als sehr gewichtiger Punkt ist eine Festlegung erforderlich die regelt, ob die Privatnutzung von E-Mails, Internet usw. erlaubt, oder generell verboten ist.
10. Das Verbot der Veränderung eingehender Mails gemäß Brief- und Fernmeldegeheimnis (Grundgesetz Art. 10) ist zu beachten bei der Kennzeichnung von als Spam erkannten Mails.
11. Es sind Regelungen zu treffen, die die Handhabung von Protokollen über den E-Mailverkehr, die Auswertung der Protokolle, die Erlaubnis zum Zugriff auf die Protokolldateien und schließlich auch die Löschrufen festlegen.
12. Die Möglichkeit zur Nutzung und die Regeln zur Handhabung von Black- und White-Lists zur Definition erwünschter Spam-Mails (z. B. Newsletter) (Whitelist) oder unerwünschter Mails (Blacklist) ist vorzusehen.

Diese nicht abschließende Sammlung von Problemen führte zu folgender BvD-AK

### **Empfehlung zum Umgang mit Spam-Mails:**

1. Alle User einer verantwortlichen Stelle sollten detailliert über die Spam-Mail Problematik informiert werden. Dies sollte die Aufforderung beinhalten im Internet restriktiv mit der eigenen E-Mail Adresse umzugehen, auf keine Spam-Mails zu antworten. Ebenso wenig sollte man die angebotene Streichung aus dem Verteiler beantragen. Die Bedeutung der false positives ist zu erklären und die entsprechende Handhabung darzulegen, die von Seiten der verantwortlichen Stelle geplanten Spam-Abwehraktivitäten sind zu erläutern und in Verbindung damit auch Aussagen zu machen über die Privatnutzung. Wird die Privatnutzung verboten, hat der Arbeitgeber uneingeschränkte

# Spam-Mail Behandlung

Zugriffsrechte, was das Filtern von Spam-Mails unproblematisch macht. Wird eine Privatnutzung erlaubt, so sind diverse Zusatzregelungen erforderlich, z. B. ist zu berücksichtigen dass je nach Art der Filterung das Fernmeldegeheimnis verletzt werden könnte, eventuell zusätzliche private E-Mail-Accounts eingerichtet werden könnten, Regelungen zur Erlaubnis für die Mail-Analyse vereinbart werden sollten, u. U. eine „Privat“-Kennzeichnung der Mails erfolgen sollte, sowie eventuelle Regelungen zum Umfang und der Art einer Privatnutzung zu treffen.

2. Eine Vereinbarung mit der Arbeitnehmervertretung ist zu treffen in der zu regeln ist:

- Privatnutzung von Internet und E-Mail
- Handhabung von Protokollen (ggf. Pseudonymisierung vornehmen)
- Speicher- bzw. Löschrufen
- Einbeziehung des Datenschutzbeauftragten in Vereinbarungen, Aktionen und Auswertungen
- Hinweis darauf, dass die Analyse nicht durch Menschen sondern elektronisch erfolgt und nur eingehende Mails analysiert werden, d.h. interner Mailverkehr ist nicht betroffen.

In Fällen, in denen keine Arbeitnehmervertretung vorhanden ist, sind solche Vereinbarungen direkt mit den Betroffenen Nutzern in schriftlicher Form zu treffen.

3. Die Auswahl eines geeigneten Filterprogramms ist zu treffen unter Berücksichtigung insbesondere der folgenden Punkte:

- Transparenz des Filterverfahrens
- hohe Trefferquote (ggf. Referenzen einholen), erforderlich zur Vermeidung von false positives
- Möglichkeit zur Definition von White- und Blacklists
- datenschutzrechtlich unbedenkliche Verfahren (d.h. z. B. mögl. anonymisierte Aufzeichnungen, Verfügbarkeit von Zugriffsregelungen mit Passwortschutz, Quarantäneordner)
- Servicegrad des Softwarelieferanten, Aktualisierungen, Zuverlässigkeit des Laufverhaltens, Konfliktfreiheit zu anderen Softwareprodukten u. ä.

4. Der BvD AK empfiehlt daher:

- Ablage der erkannten Spam-Mails in einem Quarantäneordner
- Kurzübersicht an die betroffenen Nutzer dass Spam-Mails für diese Nutzer im Quarantäneordner liegen, mit der Angabe des Absenders und der Betreffzeile. Die Nutzer mit Kundenkontakten sollten zur regelmäßigen Kontrolle (wegen der false positives) und zum Treffen von Absprachen zur Urlaubsvertretung/ Krankheitssituation verpflichtet werden.
- Regelungen zur automatischen Löschung der Mails im Quarantäneordner (wenn Punkt Urlaub/Krankheit geregelt ist, ist ein 2-3 Wochen Turnus eine gute Lösung.)

5. Die Nutzer könnten um ein regelmäßiges Feedback an den Administrator gebeten werden zu:

- Anzahl erkannte false positives
- Anzahl eingegangene false negatives
- gewünschte Eintragungen in Black- oder Whitelists

Die Feedbacks sind entsprechend auszuwerten und das Filterprogramm entsprechend anzupassen.