BREHM & v. MOERS
RECHTSANWÄLTE UND STEUERBERATER

2. Mailserver-Konferenz
18. – 20. Mai 2005

Mailfilter – mit einem Bein im Knast?

Vorgehen für eine Netzwerkpolicy

Das Problem

- Jede Mailfilterung beinhaltet die Unterbrechung einer Kommunikation. Diese Kommunikation ist zumeist durch das Fernmeldegeheimnis geschützt.
- Außerdem werden hierbei z.B. in Protokolldateien oder Filter-Ordnern personenbezogene Daten über Mitarbeiter oder Kunden gesammelt.

§ 206 StGB - Verletzung des Post- und Fernmeldegeheimnisses

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt

3. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,

2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder [...]

OLG Karlsruhe – Beschluss vom 10. Januar 2005, 1 WS 152/04

[...] 3. [...] Ein Einverständnis schließt bereits die Tatbestandsmäßigkeit des § 206 StGB aus.

[...] Ein Einverständnis kann aber nur dann von Bedeutung sein, wenn es von allen an dem konkreten Fermeldeverkehr Beteiligten erteilt wird.

OLG Karlsruhe – Beschluss vom 10. Januar 2005, 1 WS 152/04

[...] Unter Umständen kann es daher gerechtfertigt sein, eine E-Mail herauszufiltern, beispielsweise dann, wenn eine E-Mail mit Viren behaftet ist, so daß bei deren Verbreitung Störungen oder Schäden der Telekommunikations- und Datenverarbeitungssysteme eintreten.

Szenario 1 - ISPs

- Der Mailserver wird von einem Unternehmen, einer Person oder einer Organisation betrieben, die regelmäßig für Dritte E-Mails in Empfang nimmt oder versendet.

- Typische Beispiele: T-Online, AOL, JPBerlin etc.

Szenario 2 – Arbeitgeber und erlaubte E-Mailnutzung

- Der Mailserver wird von einem Unternehmen betrieben, das regelmäßig für seine Mitarbeiter E-Mails in Empfang nimmt oder versendet und den privaten Gebrauch des Internets genehmigt hat.

- Die erlaubte private Nutzung dürfte heute den Standardfall darstellen.

Szenario 3 – Arbeitsgeber und private Nutzung untersagt

- Der Mailserver wird von einem Unternehmen betrieben, das regelmäßig für seine Mitarbeiter E-Mails in Empfang nimmt oder versendet und den privaten Gebrauch des Internets untersagt hat.

- generell kann die private Nutzung untersagt werden, dies ist aber eher unüblich

Mailfilterung in Szenario 1

- ISP darf nur dann E-Mails filtern, wenn der Benutzer dies ausdrücklich gestattet hat **(STREITIG!).**
- Auch über AGB möglich (aber, § 4a BDSG sieht Schrifform vor, soweit nicht unangebracht).
- Umfang der Filterung und Funktion ist zu erklären.
- Protokolldateien sind umgehend soweit nicht mehr zur Funktionsüberprüfung oder Kostenermittlung nötig zu löschen.

Szenario 4 – öffentlich-rechtlicher Arbeitgeber

- Der Mailserver wird von einer Organisationsform der öffentlichen Hand betrieben, die regelmäßig für seine Mitarbeiter E-Mails in Empfang nimmt oder versendet.

- Typische Beispiele: Senat von Berlin, Treuhandanstalt, Bundeswehr

Mailfilter

- Mails werden gar nicht angenommen (Greylisting)
- Mails werden angenommen, aber nicht zugestellt (Black- oder Whitelisting) sondern
  a) gelöscht
  b) in einen Spam-Ordner umgeleitet
- Mails werden angenommen, mit einem Spam-Flag versehen und zugestellt
- Es wird eine Protokolldatei angelegt für 1.-3.

Mögliche Straftaten / Ordnungswidrigkeiten

- § 206 StGB – Verletzung des Post- und Fernmeldegeheimnis, insbesondere: Unterdrückung oder Weitergabe an Dritte
- §§ 43, 44 BDSG – fahrlässige und vorsätzliche Verstöße gegen das BDSG, insbesondere: Erhebung oder Speicherung von Daten ohne Zustimmung des Betroffenen
- Betroffen ist hiervon nicht nur der ISP oder der Arbeitgeber (bei Gesellschaften deren Organe) sondern auch der selbst handelnde Systemadministrator.

Zulässigkeit der Mailfilterung

- Szenario 1.: grds. nein, Verbot folgt aus dem Grundsatz des Fernmeldegeheimnisses, § 88 TKG, § 206 TKG, 28ff BDSG etc.
- Szenario 2.: siehe 1. mit Ausnahmen
- Szenario 3.: grds. zulässig, mit Ausnahmen
- Szenario 4.: je nach Erlaubnis der privaten Nutzung wie unter 2.-3.

Mailfilterung in Szenario 1

- Vorhaltung gefilterter Mails wird empfohlen – keine Löschung gem. § 206 StGB - hierfür bedarf es allerdings der ausdrücklichen Zustimmung des Kunden.

- False Positives sind durch Erweiterungen und Updates der Filtersoftware gering zu halten, da der Benutzer grundsätzlich nicht in die Filterung „echter“ E-Mails einwilligt. Bei geringer Quote fehlt es zumindest an der Strafbarkeit mangels Vorsatz wird die Quote zu hoch, droht jedoch „Eventualvorsatz“ nämlich das billigende Inkaufnehmen der Tathandlung

Mailfilterung in Szenario 2

- Arbeitgeber darf nur dann E-Mails filtern, wenn der Arbeitnehmer oder der Betriebsrat dies ausdrücklich gestattet hat.
- Gestattung durch Arbeitsvertrag oder soweit vorhanden durch Betriebsrat.
- Jede Filtermaßnahme oder Veränderung der Maßnahme ist zwingend durch den Betriebsrat zu genehmigen, vgl. § 87 BetrVG.

Mailfilterung in Szenario 2

- Protokolldateien sind umgehend, soweit sie nicht mehr zur Funktionsüberprüfung oder Kostenkontrolle nötig sind, zu löschen.

- Vorhaltung gefilterter Mails wird empfohlen, hierfür bedarf es allerdings der ausdrücklichen Zustimmung des Arbeitnehmers und soweit vorhanden des Betriebsrates.

- False Positives sind wie beim ISP zwingend niedrig zu halten.

Mailfilterung in Szenario 3

- Arbeitgeber grundsätzlich E-Mails filtern, da es sich ausschließlich um geschäftliche Kommunikation handelt, bei denen grds. keine Verletzung des Persönlichkeitsrechtes von Mitarbeiter droht.

- Jede Filtermaßnahme ist zwingend durch den Betriebsrat zu genehmigen, vgl. § 87 BetrVG.

- Protokolldateien können solange sie zur Funktionsüberprüfung oder Kostenermittlung notwendig sein aufbewahrt werden

Mailfilterung in Szenario 3

- Problematisch ist jedoch die Handhabung bei tatsächlich privater E-Mail: SEHR streitig, ob durch Filterung gefundene Mail für eine Kündigung genutzt werden darf.

- False Positives sind alleiniges Risiko des Arbeitgebers.

Mailfilterung in Szenario 4

- Behörde oder öff.-rechtl. Arbeitgeber ist so zu stellen, wie der Arbeitgeber in den Szenarien 2.-3.
- Jede Filtermaßnahme ist zwingend durch den Personalrat zu genehmigen, vgl. z.B. § 85 PersonalVG Berlin.
- Auch im öff.-rechtl. Bereich gilt der Grundsatz der Datenvermeidung, vgl. § 3a, 14 BDDSG.
- False Positive Quoten sind wie in Szenario 2. und 3. zu behandeln.

Ausnahmen

- Virenfilter sollen als Selbstschutzrecht des Arbeitgebers immer zulässig sein, dies gilt nicht bei ISPs, da die Viren dort regelmäßig nur den Computer des Nutzers betreffen.
- Zur Videoüberwachung hat das BAG Ausnahmen entwickelt: Zulässig und auch vor Gericht verwendbar sein soll die Mailüberwachung, wenn konkreter Verdacht einer Straftat vorliegt und alle anderen Mittel ausgeschöpft sind – bisher sind andere Gerichte dem sehr kritisch gegenüber getreten.

Fazit

- Mailfilter sind in jedem Fall mit den Betroffenen abzustimmen.
- Mailfilter müssen technisch immer weiter entwickelt werden.
- Änderungen der Filtersysteme sind dem Betroffenen oder dessen Vertretern mitzuteilen.
- Schon bei Verstößen gegen Formerfordernisse kann Strafbarkeit des Admins und der Geschäftsführung drohen

Nutzungspolicy für ISPs

„1. Der Benutzer stimmt der Nutzung von Mailfiltern durch den ISP zu. Die E-Mails werden dabei nach einer Liste von vorgegebenen Worten und Kombinationen gefiltert. Außerdem werden E-Mails, die Viren und schädliche Software enthalten, ebenfalls gefiltert. Der Benutzer kann jederzeit eine Mitteilung der Filterbegriffe erfragen."

Einwilligung in die Filterung und Erläuterung des Inhaltes der Filterung. Optimal wäre es wenn der Benutzer die Begriffe oder Kriterien einsehen könnte.

Nutzungspolicy für ISPs

„2. Dem Benutzer ist bekannt, daß es infolge der verwendeten Technik zu fehlerhaften Filterungen kommen kann. Der ISP wird daher die E-Mails bis zu 7 Tage aufbewahren. Während dieser Zeit kann der Benutzer die für ihn gefilterten E-Mails erfragen und herausverlangen. Nach Ablauf der Frist ist der ISP berechtigt die E-Mails zu löschen."

- False Positives können nicht ausgeschlossen werden.
- Aufbewahrung im Spam-Folder ermöglicht Kunden den Zugriff und stellt keine Unterbrechung des Fernmeldeverkehrs dar.
- Logfiles sind zu anonymisieren oder umgehend zu löschen.

Nutzungspolicy für ISPs

3. Der ISP wird den Benutzer über Veränderungen der Filtersoftware umgehend informieren.

4. Sollte der Benutzer die Zustimmung zur Filterung zurücknehmen, steht dem ISP ein sofortiges, fristloses Kündigungsrecht zu.“

Änderungen sind idealerweise vorher anzukündigen. Nur so ist gewährleistet, daß die Einwilligung des Benutzers noch gültig ist. Daran kann bei der Veränderung der Filter – in erheblichem Maß – Zweifel bestehen. Eine Filterung ohne Einwilligung ist strafbar. Daher muss der ISP kündigen können.

Nutzungspolicy für ISPs - ideale Lösung -

1. Es ist dem Benutzer möglich die Konfiguration des Filters inhaltlich nachzuvollziehen.
2. Der Benutzer kann jederzeit die gefilterten Mails einsehen, wenn er dies will.
3. Protokolldaten der Filterung werden umgehend nach der technischen Überprüfung gelöscht.
4. Die Zustimmung in die Filterung wird schriftlich erteilt. Soweit sie elektronisch erteilt wird, muss sie a) protokolliert werden, b) muss der Inhalt immer abrufbar sein, c) muss eine Einwilligung bewußt erfolgen („Häckchen“) d) muss die Einwilligung widerufbar sein.

Nutzungspolicy bei Arbeitgebern mit Betriebsrat / Personalrat

- Arbeitgeber sind verpflichtet sich der Zustimmung des Personalrats oder des Betriebsrates zu versichern. Beiden steht ein Auskunftsrecht zu. Der Datenschutzbeauftragte ist hinzuzuziehen.
- Der Arbeitgeber muss daher das gesamte System der Filterung in technischer und in untechnischer Art und Weise entweder dem Betriebsrat oder dem Personalrat vorlegen.
- Dies umfasst die Filterkriterien, die Handhabung der gefilterten Nachrichten, die Speicherzeiten sowie die Personen die zu den gefilterten Nachrichten und zu den Protokollen Zugriff haben.
- Veränderungen bedürfen einer erneuten Genehmigung soweit diese nicht völlig unwesentlich sind, wie z.B. die Veränderung einiger Worte in der Filterliste.

BREHM & v. MOERS
RECHTSANWÄLTE UND STEUERBERATER

Nutzungspolicy bei Arbeitgebern mit Betriebsrat / Personalrat - Checkliste

Vorlage an den Betriebsrat:

2. Bezeichnung der Software, Manual, Beschreibung der Funktion
3. Filterbegriffe, Kriterien
4. Beispiel der entstehenden Logfiles
5. Stellungnahme des Datenschutzbeauftragten soweit vorhanden
6. Benennung von Ansprechpartnern im Rechenzentrum/IT-Abteilung
7. Regelmäßige Berichte über Funktion und Veränderungen am System

Nutzungspolicy für Arbeitgeber ohne Betriebsrat

„Der Arbeitnehmer bestätigt mit seiner Unterschrift unter diesen Arbeitsvertrag, daß ihm bekannt ist, daß der Arbeitgeber den eingehenden E-Mailverkehr nach unerwünschter Werbung, Viren und anderen schädlichen oder unerwünschten Daten filtert. Soweit der Arbeitnehmer den Zugang privat nutzt, bzw. nutzen darf, erteilt der dem Arbeitgeber insofern die Einwilligung in die Filterung der Daten, obwohl ihm bewußt ist, daß es zu fehlerhaften Filterungen kommen kann.“

Nutzungspolicy für Arbeitgeber ohne Betriebsrat

„Darüber hinaus wird der Arbeitgeber keine Kenntnis von den gefilterten Nachrichten nehmen. Der Arbeitgeber ist befugt diese Nachrichten mit der hiermit erteilten Zustimmung des Arbeitnehmers umgehend zu löschen ohne diese aufzubewahren.“

Auch im Arbeitsrecht gilt es die gleichen Risiken wie auch beim ISP auszuschalten. Soweit rein beruflicher E-Mailverkehr betroffen ist, werden die Rechte des Arbeitnehmers jedoch weit weniger angetastet. Muster sind jedoch immer an die tatsächlichen Gegebenheiten, die Position und das zulässige Nutzungsverhalten anzupassen.

Nutzungspolicy für Arbeitgeber ohne Betriebsrat

- Für bestehende Arbeitsverhältnisse sollte eine Zustimmungserklärung wie im obigen Beispiel dringend nachträglich eingeholt werden.
- Auch hier gilt: individuelle Gestaltung je nach Arbeitsplatz und bisheriger betrieblicher Übung
- Im Zweifel: Änderungskündigung

Mailfilter – mit einem Bein im Knast
Relevante Rechtsgrundlagen

- Strafgesetzbuch – StGB (http://bundesrecht.juris.de/bundesrecht/stgb/)
- Bürgerliches Gesetzbuch – BGB (http://bundesrecht.juris.de/bundesrecht/bgb/)
- Betriebsverfassungsgesetz – BetrBG (http://bundesrecht.juris.de/bundesrecht/betrvg/)
- Telekommunikationsgesetz – TKG (http://bundesrecht.juris.de/bundesrecht/tkg/)
- Teledienstegesetz – TDG (http://bundesrecht.juris.de/bundesrecht/tdg/)
- Bundesdatenschutzgesetz – BDSG (http://bundesrecht.juris.de/bundesrecht/bdsg_1990/index.html)
- Landesdatenschutzgesetze (http://www.datenschutz-berlin.de/recht/de/dsg.htm)
- Personalvertretungsgesetze der Länder (http://www.personalvertretungsgesetz.de/)

Fragen?

- Sollten Fragen bestehen, stehe ich jedem gern zur Verfügung:
- RA Kai Bodensiek, kb@bvm-law.de
- RAe Brehm & v.Moers
  Tel.: 030 – 26 93 95 0
  Fax: 030 – 26 93 95 15