

IronPort Whitepaper

# Rechtskonforme Spamfilterung

Straf-, telekommunikations- und datenschutzrechtliche  
Aspekte der reputationsbasierten E-Mail-Filterung

Dr. Jyn Schultze-Melling LL.M. , NÖRR STIEFENHOFER LUTZ



# 1. INHALTSVERZEICHNIS

<b>2. VORWORT</b> .....	<b>3</b>
<b>3. REPUTATIONSBASIERENDE FILTERMETHODEN</b> .....	<b>4</b>
<b>4. RECHTLICHER RAHMEN FÜR DEN EINSATZ REPUTATIONSBASIERENDER FILTERMETHODEN</b> .....	<b>5</b>
Verschiedene Anforderungen für verschiedene Zielgruppen .....	5
Deutsche E-Mail-Provider .....	5
Sonstige deutsche Unternehmen.....	5
Im Ausland operierende Unternehmen und Provider .....	5
Datenschutzrechtliche Aspekte des Einsatzes reputationsbasierter Filtermethoden .....	6
Datenschutzrechtliche Grundlagen.....	6
Konsequenzen für den rechtssicheren Einsatz reputationsbasierender Filtermethoden im Unternehmen.....	7
Telekommunikationsrechtliche Aspekte der reputationsbasierten Filterung von E-Mails.....	10
Anwendbarkeit des TKG auf deutsche Provider und Unternehmen.....	10
Telekommunikationsrechtliche Grundlagen .....	10
Möglichkeiten zur Reglementierung privaten Nutzung betrieblicher Kommunikationsmittel.....	11
Strafrechtliche Aspekte.....	12
Grundlagen.....	12
Konsequenzen für den Einsatz reputationsbasierender Filtermethoden im Unternehmen.....	13
<b>5. FREQUENTLY ASKED QUESTIONS ZUR RECHTSSICHEREN GESTALTUNG DER E-MAIL-FILTERUNG MITTELS REPUTATIONSBASIERTER FILTERSYSTEME</b> .....	<b>15</b>
Ist der Einsatz von reputationsfilterungs-techniken rechtlich unbedenklich?.....	15
Wie müssen die Systeme aufgesetzt werden, um datenschutzrechtlich konform zu sein? .....	15
Was hat das Fernmeldegeheimnis mit Spam-Filterung zu tun? .....	15
Macht man sich durch den Einsatz von E-Mail-Filtern strafbar? .....	15
Was bewirkt eine Einwilligung der Mitarbeiter in die Filterung?.....	16

## 2. VORWORT

Die Flut unerwünschter E-Mail-Werbung und virenverseuchter E-Mails nimmt stetig zu. Die regelmäßig veröffentlichten Zahlen des IronPort Threat Operation Center (TOC) zeigen, dass 80 % des weltweiten E-Mail-Aufkommens aus unerwünschten E-Mails bestehen. Zwei von drei E-Mails sind Werbung, und jedes Jahr wächst die Spam-Summe um über 100 %. Außerdem besteht bei jeder empfangenen E-Mail eine statistische Chance von 3 %, einen - möglicherweise höchst gefährlichen - Virus auf den Rechner herunterzuladen.

Besonders Unternehmen sind diesen Problemen ausgeliefert, da sie mitunter höchst lukrative Ziele für Angriffe bieten. Neben den Bedrohungen durch Viren und andere elektronische Schädlinge geht vor allem Arbeitszeit verloren, wenn die Mitarbeiter erwünschte von unerwünschten E-Mails trennen müssen. Automatische Spamfilter versprechen Erleichterung: Sie nehmen den Menschen die Arbeit ab, indem sie eingehende Post automatisch sortieren und Spam löschen. Durch den Einsatz einer entsprechenden Anti-Spam-Appliance kann dieser Gefahr effektiv begegnet werden.

Will sich ein Unternehmen auf diese Weise von unerwünschten E-Mails schützen, ist jedoch Umsicht bei der Auswahl und der Konfiguration des geeigneten Filtersystems geboten. Denn bei aller Bequemlichkeit ist nicht jede Filterlösung und jede mögliche Konfiguration rechtlich unbedenklich. Herkömmliche Systeme kollidieren häufig mit strafrechtlichen, datenschutzrechtlichen und telekommunikationsrechtlichen Vorschriften. Auslöser dieser Probleme können die Funktionsweise des Systems, aber auch Konfigurationsfehler sein.

Dieses Whitepaper soll zunächst kurz am Beispiel der IronPort-Appliances die technische Funktionsweise der innovativen reputationsbasierenden Filtermethoden aufzeigen. Hiernach folgt eine rechtliche Analyse der einzelnen Funktionen. Den Abschluss bildet eine FAQ, die die wichtigsten Fragen zum Einsatz reputationsbasierender Filtermethoden auf einen Blick beantwortet.

### 3. REPUTATIONSBASIERENDE FILTERMETHODEN

Viele Spam-Wellen verbreiten sich vor allem deshalb so schnell, weil sie durch die herkömmlichen Spam-Filter schlüpfen können. Diese fokussieren rein auf textliche Inhalte und versuchen anhand von Schlüsselwörtern die E-Mail zu kategorisieren. Manche Angreifer transportieren aber mittlerweile ihren Spam über geschickt getarnte Weblinks in E-Mails. Diese verweisen dann lediglich auf eine bestimmte Website, von der aus Spam und immer häufiger zugleich auch Computerviren und andere Malware automatisch heruntergeladen wird. Vor allem durch Schwachstellen von weit verbreiteten Browser-Programmen konnten sich solche schädliche Informationen rasant verbreiten.

Weitere Komplexität bieten solche Nachrichten, bei denen der Inhalt nicht als Text, sondern fast ausschließlich als Bild vorliegt: die herkömmlichen Filter können diese Informationen nicht verlässlich verarbeiten. Hinzukommt, dass auch die Bilder gefährliche Links transportieren können. Die Zahl dieser Image-Spam-Mails ist in der letzten Zeit förmlich explodiert: Während im Oktober 2005 lediglich 4,8 Prozent der gesamten Spam-Flut Bilddateien waren, stieg der Anteil bis April 2007 bereits auf ein Drittel des gesamten Spam-Aufkommens. Das bedeutet, dass täglich 25 Milliarden derartiger Nachrichten versendet werden. Mit jeder Spam-Attacke verändern sich die meisten Bilder zudem minimal, um herkömmliche Spam-Blocker auszuhebeln.

Angesichts der neuartigen Bedrohungen des Netzes bieten herkömmliche rein inhaltsbasierte Filter keinen ausreichenden Schutz. Dieser rein reaktive Schutz ist dazu verurteilt, der aktuellen Bedrohungslage stets um Stunden oder sogar Tage hinterher zu hinken. Reputationsbasierte Filtertechnologien versuchen stattdessen, eine möglichst objektive Einschätzung der Seriosität einer Website oder eines Sendersnetzwerkes zu erhalten. Diese Einschätzung ist in vielen Fällen bereits verfügbar, wenn ein Angriff gerade erst beginnt, denn spezielle zentrale Datenbanken analysieren ständig eine Unmenge an technischen Parametern für mehr als 25 Prozent des weltweiten E-Mail-Aufkommens. Diese Informationen können abgefragt werden, bevor der eigentliche E-Mail-Übertragungsvorgang beginnt und ermöglichen es, über zwei Drittel der unerwünschten Daten zu vermeiden, indem das sendende System bereits im Vorfeld abgewiesen wird.

Dieses System ist jedoch nicht nur technisch hochkomplex und ebenso effizient, sondern birgt auch nicht zu unterschätzende rechtliche Risiken, denen sich der Verwender bewusst sein muss. Bei derartigen Anti-Spam-Lösungen ist es wie mit der Benutzung von Hochtechnologie im Allgemeinen: Durch eine entsprechende Handhabung lassen sich die Haftungspotentiale minimieren oder sogar ganz ausschließen. Dieses Whitepaper wird die rechtlichen Grundlagen darstellen, die einen rechtskonformen Einsatz der Appliances ermöglicht.

## 4. RECHTLICHER RAHMEN FÜR DEN EINSATZ REPUTATIONSBASIERENDER FILTERMETHODEN

### VERSCHIEDENE ANFORDERUNGEN FÜR VERSCHIEDENE ZIELGRUPPEN

Eine Schwierigkeit im Zusammenhang mit dem rechtskonformen Einsatz von reputationsbasierten Anti-Spam-Lösungen ist, dass nicht für jeden Nutzer derselbe rechtliche Rahmen gilt. Bevor also eine Aussage zur Rechtmäßigkeit des Einsatzes dieser Systeme getroffen werden kann, muss also zunächst zwischen verschiedenen Verwendergruppen differenziert werden.

#### DEUTSCHE E-MAIL-PROVIDER

Auf E-Mail-Provider mit Sitz in Deutschland ist deutsches Recht ohne Einschränkungen anwendbar. Aus diesem Grund unterliegen sie als datenverarbeitende Stelle dem Bundesdatenschutzgesetz (BDSG) und als Telekommunikationsanbieter dem Telekommunikationsgesetz (TKG). Für den Provider handelnde und verantwortliche Personen müssen sich außerdem nach den Vorschriften des Strafgesetzbuchs (StGB) richten.

#### SONSTIGE DEUTSCHE UNTERNEHMEN

Bei sonstigen inländischen Unternehmen muss zwischen zwei Gruppen unterschieden werden: Gestattet ein Unternehmen seinen Mitarbeitern, die zur Verfügung gestellten Telekommunikationsmittel für private Zwecke zu nutzen, wird es nach geltender Rechtsprechung wie ein Provider behandelt und ist daher in seinen Pflichten der Gruppe der Provider gleichgestellt. Einschlägig sind also wiederum das BDSG, das TKG sowie das StGB.

Ist den Mitarbeitern hingegen eine Privatnutzung per Betriebsvereinbarung oder per arbeitsvertraglicher Regelung untersagt, wird das Unternehmen nicht als Provider angesehen und unterliegt daher auch nicht den besonderen Bestimmungen für Telekommunikationsanbieter. In diesem Fall findet also das TKG keine Anwendung. Das BDSG und das StGB sind jedoch weiterhin zu beachten. Hierzu erfahren Sie später im Zusammenhang mit den telekommunikationsrechtlichen Aspekten der Reputationsfilterung mehr.

#### IM AUSLAND OPERIERENDE UNTERNEHMEN UND PROVIDER

Grundsätzlich unterliegen im Ausland ansässige Unternehmen und Provider nicht deutschem Recht. Sobald diese Unternehmen jedoch in Deutschland tätig werden, berühren sie den nationalen Rechtskreis und müssen gegebenenfalls die entsprechenden Gesetze berücksichtigen. Hierbei gelten die folgenden Regeln:

##### *Anwendbarkeit des BDSG*

Ausländische Unternehmen, die in Deutschland Daten erheben, verarbeiten oder nutzen, haben unter Umständen das BDSG zu beachten. Dies gilt gemäß § 1 Abs. 5 BDSG für im Europäischen Wirtschaftsraum (EWR) ansässige Unternehmen, die in Deutschland eine Niederlassung haben (ansonsten gilt das Datenschutzrecht des Landes, in dem das Unternehmen seinen Sitz hat). Für ausländische Unternehmen außerhalb des EWR gilt das BDSG ohne Rücksicht auf deutsche Niederlassungen.

---

## Anwendbarkeit des StGB

Nach dem sog. „Ubiquitätsprinzip“ gilt eine Straftat als in Deutschland begangen, wenn der Täter dort gehandelt hat oder der Taterfolg dort eingetreten ist. Liegt eine dieser Voraussetzungen vor, ist deutsches Strafrecht anwendbar. Unterhält zum Beispiel ein ausländisches Unternehmen in Deutschland einen Server mit einem Filtersystem, unterliegen Straftaten, die im Einflussbereich dieses Servers begangen werden, deutschem Strafrecht.

---

## Anwendbarkeit des TKG

Nach der Legaldefinition in § 3 Nr. 22 TKG betrifft das TKG den technischen Vorgang des Aussendens, Übermittels und Empfangens von Signalen mittels Telekommunikationsanlagen durch TK-Dienstleister in Deutschland. Damit gilt im TK-Recht das sog. „Territorialitätsprinzip“.

# DATENSCHUTZRECHTLICHE ASPEKTE DES EINSATZES REPUTATIONSBASIERTER FILTERMETHODEN

---

## DATENSCHUTZRECHTLICHE GRUNDLAGEN

Das Bundesdatenschutzgesetz (BDSG) ist das zentrale Regelwerk für den Umgang mit personenbezogenen Daten von natürlichen Personen. Es dient in erster Linie dazu, das verfassungsmäßige Recht natürlicher Personen auf informationelle Selbstbestimmung zu schützen. Dies ist das Recht, grundsätzlich selbst über die Verwendung personenbezogener Daten entscheiden zu dürfen. Es ist Ausdruck des allgemeinen Persönlichkeitsgrundrechts.

Personenbezogene Daten sind dabei nach der Definition des § 3 Abs. 1 BDSG „*Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person*“. Die Daten müssen also nicht namentlich zugeordnet sein. Es reicht vielmehr aus, wenn der Personenbezug ohne allzu großen Aufwand aus den Daten hergeleitet werden kann. Im Falle von IP-Adressen haben die Gerichte mehrfach entschieden, dass diese – wenn sie einer natürlichen Person zugeordnet werden können – durchaus personenbezogene Daten im Sinne des Datenschutzrechtes sein können.

Die grundlegende Maxime für das gesamte deutsche Datenschutzrecht ist das Prinzip des Verbots mit Erlaubnisvorbehalt. Aufgrund dieses Prinzips dürfen personenbezogene Daten grundsätzlich nicht erhoben, verarbeitet oder genutzt werden. Ausnahmen gibt es folglich nur dann, wenn entweder ein ausdrückliches und freiwilliges Einverständnis des Betroffenen in den Datenverarbeitungsvorgang vorliegt oder aber eine gesetzliche Erlaubnisregelung existiert. Da das Einverständnis des Betroffenen nach § 4 a BDSG informiert und in der Regel schriftlich erteilt werden muss, muss es innerhalb eines Unternehmens entweder von jedem Mitarbeiter einzeln eingeholt werden, oder durch eine entsprechende Betriebsvereinbarung für alle Mitarbeiter verbindlich geregelt werden.

Gesetzliche Erlaubnistatbestände wiederum können sich aus dem BDSG selbst oder aus spezialgesetzlichen Regelungen ergeben. Hierbei sind in erster Linie die §§ 28 und 29 des BDSG und entsprechende Regelungen im Sozialgesetzbuch, im TKG oder im Verwaltungsrecht einschlägig. Verantwortlich für die Einhaltung dieser Vorschriften ist dabei nach § 3 Abs. 7 BDSG stets die Stelle, die die Daten für sich selbst oder durch andere

als deren Auftraggeber erhebt, verarbeitet oder nutzt, also im Falle von datenverarbeitenden Spam-Filtern das Unternehmen, dass diese einsetzt, und nicht etwa der Hersteller der Appliance.

## KONSEQUENZEN FÜR DEN RECHTSSICHEREN EINSATZ REPUTATIONSBASIERENDER FILTERMETHODEN IM UNTERNEHMEN

Aus datenschutzrechtlicher Sicht stellen sich daher beim Einsatz reputationsbasierender Filtersysteme zwei Problembereiche. Erstens stellt sich natürlich die Frage, wie die Kontrolle und Filterung ein- und ausgehender E-Mails datenschutzrechtlich einzuordnen ist, also ob eine Einwilligung oder ein gesetzlicher Erlaubnisatbestand erforderlich sind. Darüber hinaus ist aber auch zu prüfen, ob bei einer Teilnahme an der 'SenderBase Network Participation' oder ähnlichen 'Feedback-Mechanismen' durch Übermittlung bestimmter Informationen an die Betreiber der zentralen Reputationsdatenbanken datenschutzrechtliche Regeln zu beachten sind.

### *Kontrolle und Filterung von E-Mails*

Um die Funktionalität des Systems auszunutzen, müssen sowohl eingehende als auch ausgehende E-Mails die Barrieren der Appliances durchlaufen. Ausgehende E-Mails werden dabei keiner inhaltlichen Kontrolle unterzogen, sondern lediglich - je nach Einstellung - auf Viren-Signaturen hin überprüft. Hierbei werden in der Regel keine personenbezogenen Daten verarbeitet. Eingehende E-Mails werden dagegen zweistufig auf ihren Schadcharakter und auf Spam hin untersucht:

Auf der ersten Stufe übermittelt die Appliance die IP-Adresse des versendenden E-Mail-Netzwerks an die zentrale Reputationsdatenbank (etwa der IronPort SenderBase-Datenbank). Ausschlaggebend hierbei ist der Umstand, dass diese IP-Adresse dabei auf Protokoll-Ebene zwischen dem Sender- und dem Empfängersystem ausgetauscht wird, bevor es zu einem eigentlichen Verbindungsaufbau kommt. Zudem ist sie in aller Regel keiner bestimmten natürlichen Person zugewiesen, sondern dem E-Mail-Gateway des Sendersystems, so dass hier kein Personenbezug möglich ist und daher keine personenbezogenen Daten im Sinne des BDSG vorliegen. In der Reputations-Datenbank wird die vom Empfängersystem übermittelte IP-Adresse des Sendersystems auf einen dort hinterlegten Reputationswert überprüft; existiert ein solcher Wert, wird er der Appliance mitgeteilt. Wie diese den ihr übermittelten Wert einordnet und welche Schlussfolgerungen sie daraus für den Umgang mit den ihr angebotenen E-Mail zieht, bleibt dabei vollkommen dem Verwender der Appliance vorbehalten. In den meisten Fällen wird dieser aber E-Mails mit Reputationswerten unter einer bestimmten im Voraus festgelegten Marke ablehnen. Beherzigt er die Höflichkeitsregeln, wird der Verwender seine Appliance so konfigurieren, dass diese das Sendersystem wissen lässt, dass und warum sie keine E-Mails von diesem annehmen wird. Unterschreitet der Reputationswert einen sehr niedrigen Wert, können derartige Verbindungsversuche aber auch einfach sang- und klaglos abgelehnt werden.

Passiert die E-Mail den Reputationsfilter, wird sie auf der zweiten Stufe einer inhaltlichen Prüfung unterzogen. Im Rahmen dieser Prüfung werden unter Umständen personenbezogene Daten verarbeitet. Die Virusprüfung läuft dabei - wie auch bei ausgehenden E-Mails - in der Regel ohne Zugriff auf möglicherweise personenbezogene Daten ab. Vielmehr untersucht der Virenschanner Anhänge auf schadhafte Software, ohne dabei auf den Text der E-Mail zuzugreifen. Auch dieser Schritt ist daher datenschutzrechtlich unbedenklich. Die Spamprüfung hingegen erhebt und nutzt unter Umständen personenbezogene Daten des Inhalts, beispielsweise im Header oder im Textkörper vorhandene Namen. Hierbei kommt es nicht darauf an, ob ein Mensch diese Daten zur Kenntnis nimmt, etwa ein IT-Mitarbeiter des die E-Mail empfangenden Unternehmens.

Für dieses Verfahren ist also in der Regel eine datenschutzrechtliche Erlaubnis erforderlich. Die Einholung einer Einwilligung der Betroffenen nach § 4 a BDSG ist aber oftmals praktisch nicht durchführbar, weil auch potentiell vorhandene Daten des (möglicherweise gar nicht bekannten) Versenders der E-Mail in die Prüfung einbezogen werden. Ohne eine Einwilligung bedarf eine Datenverarbeitung eines gesetzlichen Erlaubnistatbestandes. Nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist eine Erhebung und Nutzung dann zulässig, wenn sie zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist. „Berechtigt“ ist dabei grundsätzlich jedes Interesse, das die Rechtsordnung billigt, wozu auch das Interesse des Unternehmens an störungsfreier Kommunikation zählt. Da die automatische Spamfilterung im Vergleich zu anderen Varianten (insbesondere persönlicher Durchsicht aller E-Mails durch einen Dritten) zudem einen relativ geringen Eingriff bedeutet und in den meisten Fällen auch keine weniger invasiven Mittel denkbar sind, ist die Maßnahme regelmäßig auch „erforderlich“.

Aber selbst, wenn eine Maßnahme berechtigten Interessen dient und zudem erforderlich ist, muss dennoch eine Abwägung der Interessen des Unternehmens mit den Interessen des von der Maßnahme Betroffenen stattfinden. Hierbei muss sich ein Übergewicht zugunsten der verantwortlichen Stelle ergeben. Im Falle der Verarbeitung von Spam-Emails ist also Interesse des Unternehmens oder des Providers an der Spamfilterung sowohl gegen die Interessen des Empfängers als auch gegen die Interessen des Versenders der E-Mail abzuwägen. Die Interessen des Versenders einer Spam-Mail sind in diesem Zusammenhang nur niedrig einzustufen. Geht man von der Prämisse aus, dass unter „Spam“ nur unerwünscht zugesandte Werbung verstanden wird, verstößt der Versand derartiger Nachrichten regelmäßig gegen datenschutz- oder wettbewerbsrechtliche Vorschriften. Dieses Interesse des Versenders wird die Interessen der Empfänger, der Versender „ordnungsgemäßer“ E-Mails und vor allem das Interesse eines Unternehmens an einem ungestörten Arbeitsablauf seiner Mitarbeiter und der Freihaltung des Kommunikationssystems von Belastung durch übermäßiges Nachrichtenaufkommen kaum überwiegen können.

---

### *Die Übermittlung gewonnener Daten an Hersteller wie IronPort zur Teilnahme an der Reputationswert-Erstellung am Beispiel der SenderBase Network Participation*

Die Teilnahme am SenderBase Network ist schon im Interesse des Unternehmens selbst sinnvoll, um ein Höchstmaß an Schutz zu erhalten. Darüber hinaus trägt ein Unternehmen zur Sicherung der elektronischen Kommunikation weltweit bei. Hiervon profitieren nicht zuletzt die Geschäftspartner, die auf der anderen Seite regelmäßig zu den ersten Geschädigten zählen, wenn sich ein Virus an alle Kontakte eines Adressbuchs versendet. Die Datenübermittlungsfunktion kann dennoch jederzeit ohne weitere Konsequenzen abgeschaltet werden. Die Appliance überträgt in diesem Fall keinerlei Informationen an IronPort. Ist die Übertragungsfunktion jedoch aktiviert, werden bestimmte Daten an die Server der Herstellerfirma IronPort übermittelt. Die übermittelten Daten lassen sich in Appliance-bezogene und IP-bezogene Daten unterteilen.

Appliance-bezogene Daten sind solche Daten, die sich einer bestimmten Appliance zuordnen lassen. Neben Angaben zu deren Status selbst werden ausschließlich Einstellungsparameter erhoben. Hierzu gehören insbesondere

- der MGA-Identifizier,
- der Zeitpunkt der Übermittlung,
- die Software-Version,
- die Rule Set Version Numbers,

- das Update-Intervall der Antivirus-Software,
- die Größe des Quarantäne-Ordners,
- die Anzahl der im Quarantäne-Ordner befindlichen E-Mails,
- der Reputationswert, ab dem E-Mails in den Quarantäne-Ordner geleitet werden,
- die Höhe der summierten Grenzwerte aller E-Mails in Quarantäne,
- die maximale Quarantäne-Dauer,
- die Anzahl der E-Mails, die in Quarantäne geschickt wurden, sortiert nach Angabe des Grundes (z.B. wegen eines .exe-Anhangs), und aus der Quarantäne entlassen (z.B. manuelle Freigabe) wurden, im Zusammenhang mit den Virensan-Ergebnissen,
- die Anzahl der E-Mails, bei denen bei der Entlassung aus der Quarantäne jeweils eine bestimmte Aktion durchgeführt wurde (z.B. Entfernen des Anhangs), sowie
- die Gesamtzeit, während der sich je E-Mails in Quarantäne befanden

IP-bezogene Daten dagegen sind solche Daten, die sich einer bestimmten IP-Adresse zuordnen lassen. Hierzu gehören insbesondere:

- die Anzahl der E-Mails, die von der jeweiligen Appliance als Spam oder verseucht erkannt wurden,
- die summierten Reputationswerte aller E-Mails, die als Spam oder verseucht erkannt wurden,
- die Anzahl der E-Mails, die verschiedene Kombinationen von Spam- oder Virus-Regeln erfüllen,
- die Gesamtsumme aller Empfänger und aller ungültigen Empfängeradressen,
- ein aus dem Namen eines Dateianhangs gebildeter Hashwert (einseitiger MD5-Hash), falls vorhanden,
- der anonymisierte Name eines Dateianhangs, falls vorhanden,
- falls vorhanden: die in den E-Mails enthaltene URLs (nur das Hauptverzeichnis, z.B. www.beispieldomain.de),
- falls vorhanden: der anonymisierte Pfad unterhalb der Domain (z.B. www.beispieldomain.de/aaa000aa/aa00aaa),
- die Gesamtanzahl der auf Spam und Viren jeweils positiv bzw. negativ getesteten E-Mails,
- die Anzahl der Dateianhänge aller E-Mails innerhalb bestimmter Größenbereiche,
- eine Liste aller in E-Mails gefundenen Dateitypen,
- eine Liste der Dateitypen aller Anhänge, deren tatsächlicher Dateityp nicht mit dem Dateinamen übereinstimmt oder sich in einem Archiv befindet, sowie
- die Summe gefundenen Dateien eines tatsächlichen Dateityps innerhalb eines bestimmten Größenbereichs.

All diese Daten haben gemeinsam, dass sie keinerlei Aussagen über bestimmte natürliche Personen enthalten und auch keinen Bezug auf bestimmte natürliche Personen zulassen. Besteht eine derartige Gefahr (z.B. bei personalisierten URLs), wird durch eine Verschlüsselung die Anonymität der Daten gewährleistet. Die Erhebung, Verarbeitung und Übertragung dieser Daten an die Server der Herstellerfirma IronPort unterliegt also nicht den Bestimmungen des BDSG. Folglich bedarf es keiner datenschutzrechtlichen Genehmigung, um rechtskonform an der SenderBase Network Participation teilzunehmen. Im Gegenteil: Nicht zuletzt stellt auch die Erhöhung des allgemeinen Datenschutz-Niveaus durch Sicherung der elektronischen Kommunikation vor Spam- und Virenmails einen positiven Zusatzeffekt der Mailkontrolle dar.

## TELEKOMMUNIKATIONSRECHTLICHE ASPEKTE DER REPUTATIONSBASIERTEN FILTERUNG VON E-MAILS

### ANWENDBARKEIT DES TKG AUF DEUTSCHE PROVIDER UND UNTERNEHMEN

Bei Providern ist die Lage einfach: da sie in aller Regel Dritten gegenüber Dienstleistungen aus dem Telekommunikationsbereich erbringen, ist das TKG auf sie ohne weiteres anwendbar. Bei Unternehmen muss differenziert werden. Ob ein sich Unternehmen TKG-konform verhalten muss, richtet sich nach herrschender Rechtsprechung danach, ob es seinen Mitarbeitern Telekommunikationsmittel (z.B. E-Mail) zur privaten Nutzung bereitstellt. In diesem Fall gehen die Juristen davon aus, dass diese Arbeitnehmer „Dritte“ sind, denen das Unternehmen dann als Telekommunikationsanbieter TK-Leistungen anbietet. Das Anbieten von derartigen Leistungen kann unter anderem durch eine ausdrückliche Nutzungserlaubnis des Arbeitgebers geschehen. Zwingend ist dies jedoch nicht, denn eine private Nutzung kann auch als stillschweigend gestattet gelten. Weiß und duldet ein Unternehmen nämlich über einen gewissen Zeitraum, dass seine Mitarbeiter private E-Mails versenden, stellt dies eine entsprechende Erlaubnis in Form einer so genannten betrieblichen Übung dar.

Im Falle einer solchen Nutzungserlaubnis gilt das Unternehmen als Anbieter von Telekommunikationsdiensten nach § 3 Nr. 6 TKG und ist verpflichtet, das TKG zu beachten. Dies gilt auch für Anbieter, die nicht gegen Entgelt tätig sind. Ausreichend für den Status als Telekommunikationsanbieter ist auch bereits eine kostenlose Erbringung der Dienstleistungen, wenn dies nicht nur vorübergehend geschieht. Untersagt ein Unternehmen seinen Angestellten dagegen die private Internetnutzung und setzt diese Regelung auch konsequent durch, gilt es nicht als Anbieter von Telekommunikationsdienstleistungen. Die Vorschriften des TKG sind dann nicht anwendbar.

### TELEKOMMUNIKATIONSRECHTLICHE GRUNDLAGEN

Provider und solche Unternehmen, die ihren Angestellten die private Internetnutzung gestatten, sind also zur Einhaltung der Vorschriften des TKG verpflichtet. Dies bedeutet unter anderem, dass sie nach § 88 Abs. 2 TKG das grundgesetzlich und strafrechtlich geschützte Fernmeldegeheimnis zu wahren haben. Die Umsetzung dieses Schutzauftrags wirkt sich auf den Einsatz reputationsbasierender Filtermethoden unterschiedlich aus. Zu unterscheiden ist hier zwischen der Abwehr von Viren und der Abwehr von Spam.

#### *Zulässigkeit der Virenabwehr*

Die Filterung virenverseuchter E-Mails ist telekommunikationsrechtlich gesehen recht unbedenklich. Nach § 109 Abs. 1 TKG muss jeder Telekommunikationsdiensteanbieter zum Schutz des Fernmeldegeheimnisses

sowie des Telekommunikationssystems selbst geeignete Schutzmaßnahmen ergreifen. Viren, Spyware und sonstiger schädlicher Code sind nachweislich mehr als geeignet, sowohl die Integrität des Systems als auch die Einhaltung des Fernmeldegeheimnisses zu gefährden. Das Überprüfen des E-Mail-Verkehrs und das Löschen verseuchter E-Mails stellt in diesem Zusammenhang daher nach einhelliger Meinung keine Verletzung des Fernmeldegeheimnisses dar.

---

### *Zulässigkeit der Spamfilterung*

Unabhängig von den volkswirtschaftlichen Konsequenzen der Spam-Plage gilt unter Juristen, dass von Spam-Mails (zumindest von „reinem“ Spam ohne Spoofing) nicht die gleiche konkrete Gefahr ausgeht, wie von Viren. Die Pflicht zum Schutze der technischen Einrichtungen kann daher im Falle von Spam-Mails leider nicht zur Überwindung des Fernmeldegeheimnisses erhalten. Auch andere gesetzliche Rechtfertigungsmöglichkeiten existieren nicht. Die Spamabwehr darf also nicht ohne weiteres auf lediglich gesetzlicher Grundlage durchgeführt werden. Vielmehr ist eine Einwilligungserklärung des jeweils betroffenen Nutzers notwendig (hierzu später).

---

### *Konsequenzen für das Unternehmen*

Die Bundesnetzagentur als Regulierungsbehörde überwacht die Einhaltung der Vorschriften zum Schutz des Fernmeldegeheimnisses. Dem Unternehmen selbst drohen bei Verstößen gegen telekommunikationsrechtliche Vorschriften zudem Weisungs- und Zwangsmaßnahmen durch die Bundesnetzagentur. Sie hat gemäß § 126 TKG das Recht, Unternehmen zur Abhilfe von Verstößen anzuhalten und bei einer Weigerung selbst die notwendigen Maßnahmen anzuordnen. Diesen Anordnungen kann mit Zwangsgeldern von bis zu 500.000 Euro Nachdruck verliehen werden. Im äußersten Fall kann sogar die Betreibertätigkeit vollständig untersagt werden.

Zudem stellt jeder Verstoß gegen das Fernmeldegeheimnis eine Straftat nach § 206 StGB dar und ist daher mit Geldstrafe oder Freiheitsstrafe von bei zu fünf Jahren bedroht. Diese strafrechtlichen Konsequenzen richten sich dabei nicht gegen das Unternehmen selbst, sondern gegen seine Angestellten und Führungskräfte. Vor dem Hintergrund dieser Drohkulisse sollte demnach die private Nutzung von E-Mail und Internet untersagt und entsprechende Überwachungsmechanismen zur Kontrolle der Einhaltung dieses Verbotes etabliert werden.

---

## MÖGLICHKEITEN ZUR REGLEMENTIERUNG PRIVATEN NUTZUNG BETRIEBLICHER KOMMUNIKATIONSMITTEL

Als Mittel der Wahl kommen hierzu zum einen Vereinbarungen mit allen Arbeitnehmern in den Arbeitsverträgen in Betracht. Besteht ein Betriebsrat ist jedoch möglicherweise eine Betriebsvereinbarung, die alle Arbeitnehmer verpflichtet und keine Ergänzung der einzelnen Verträge erfordert, praktischer in der Handhabung. Übrigens: Existiert im Unternehmen ein Betriebsrat, ist dieser nach § 87 Abs. 1 des Betriebsverfassungsgesetzes mitbestimmungsberechtigt, wenn Maßnahmen zur Reglementierung der Internetnutzung ergriffen werden sollen. Zu diesen Maßnahmen zählt prinzipiell auch die Einführung eines Spamfilters. Hierbei kommt es nicht auf den Willen des Arbeitgebers an, sondern lediglich auf die technische Möglichkeit einer derartigen Nutzung. Liesse sich eine Appliance also zum Beispiel durch entsprechende Reportingfunktionalitäten dazu benutzen, die Leistung oder das Arbeitsverhalten einzelne Mitarbeiter zu kontrollieren, muss vor der Einführung derartiger Technologien der Betriebsrat um entsprechende Zustimmung gebeten werden. Kein Mitspracherecht besteht nach neuester Rechtsprechung jedoch, wenn die Privatnutzung voll-

ständig untersagt werden soll (vgl. hierzu OLG Hamm, MMR 2006, 700) – die Diskussionen mit den Betriebsräten beziehen sich also nur noch auf das ‚Wie‘ der Kontrolle eines Verbotes, nicht auf das ‚Ob‘ des Verbotes selbst.

Ein vollständiges Verbot privater Internet- und E-Mailnutzung mag aus unternehmenspolitischer Sicht eine ungünstige Lösung sein, bedeutet für das Unternehmen jedoch die sicherste Rechtsposition. Neben der Vermeidung der Anwendbarkeit des TKG bietet ein solches Verbot weitere Vorteile: Wird ein Computer ausschließlich dienstlich genutzt, hat der Arbeitgeber unbeschränkten Zugriff auf die gespeicherten Daten. Bei gestatteter Privatnutzung ist ein Zugriff auch auf gespeicherte Dateien wegen des Fernmeldegeheimnisses nur eingeschränkt möglich. Als Kompromisslösung könnten im Unternehmen beispielsweise zusätzliche Computer aufgestellt werden, die autark vom restlichen Netzwerk betrieben werden und der Kontrolle des Filtersystems entzogen sind. Diese Lösung befreit einerseits das Unternehmen hinsichtlich der Arbeitsrechner von den Regeln des TKG und trägt andererseits zu einem positiven Unternehmensklima bei, weil den Arbeitnehmern ein Internetzugang zur privaten Nutzung bereitgestellt wird.

## STRAFRECHTLICHE ASPEKTE

### GRUNDLAGEN

Unabhängig von der Eigenschaft des Anbieters von Kommunikationsdienstleistungen ist der Einsatz reputationsbasierender Filtermethoden bei Unternehmen wie Providern unter Umständen auch aus strafrechtlicher Sicht ein sensibleres Thema. Zu beachten sind hierbei vor allem zwei Vorschriften: die §§ 206 und 303a StGB.

#### § 206 StGB

Nur für Unternehmen mit gestatteter Privatnutzung und Provider potentiell gefährlich ist § 206 StGB, der die Verletzung des Fernmeldegeheimnisses unter Strafe stellt. Ist ein Unternehmen kein TK-Anbieter, ist es von dieser Vorschrift nicht betroffen, da sämtliche empfangenen E-Mails als dienstlich bedingt angesehen werden. Die Norm schützt das Fernmeldegeheimnis, das nach Art. 10 GG Grundrechtsstatus genießt. Es umfasst dabei nicht nur die „klassische“ Telefonie, sondern auch andere Kommunikationsformen wie SMS, Telefax oder E-Mail. Geschützt sind nach § 88 TKG zudem sowohl der Inhalt des Telekommunikationsvorgangs selbst, als auch dessen nähere Umstände. Hierzu zählt nach dem Willen des Gesetzgebers insbesondere auch die Telekommunikation an sich, so dass jeder Beteiligte an einem Telekommunikationsvorgang den Schutz von Art. 10 Abs. 1 GG genießt.

Tathandlung des § 206 StGB ist das unbefugte Unterdrücken einer zur Übermittlung anvertrauten Sendung gemäß § 206 Abs. 2 Nr. 2 StGB. Unterdrücken bedeutet im Rahmen des Versendens einer E-Mail, dass die E-Mail den Empfänger nicht, nicht vollständig oder erst mit einiger Zeitverzögerung erreicht.

#### § 303 a StGB

Für alle Unternehmen und Provider ist der Tatbestand der Datenveränderung nach § 303 a StGB relevant. Schutzgegenstand dieser Norm sind die Integrität von Daten und das Vertrauen des Verfügungsberechtigten, dass die gespeicherten Informationen nicht durch unberechtigte Handlungen Dritter in ihrer Verwendbarkeit beeinträchtigt werden. Untersagt ist unter anderem, Daten zu unterdrücken (was in diesem Zu-

sammenhang bedeutet, die Daten dem Zugriff des Berechtigten vorübergehend oder auf Dauer zu entziehen) und Daten zu löschen.

§ 303 a StGB unterscheidet sich in seiner Reichweite von § 206 Abs. 2 StGB in zwei Punkten: zum ersten umfasst er potentielle Täter aller Unternehmen und Provider, da seine Reichweite mangels Bezug zum Fernmeldegeheimnis nicht auf Anbieter von TK-Leistungen beschränkt ist. Zum zweiten ist der Versender einer E-Mail in weit geringerem Maße geschützt. Während der Schutz des Versenders sich beim Fernmeldegeheimnis auf den gesamten Telekommunikationsvorgang bezieht, richtet sich die Schutzdauer bei § 303 a StGB nach der Verfügungsbefugnis über die jeweiligen Daten. Schickt der Versender eine E-Mail ab, erlöschen seine Verfügungsbefugnis und damit der Schutz der Norm. Bei der Filterung vor Übertragung einer E-Mail auf das Empfängersystem ist also auf die Interessen des Versenders keine Rücksicht mehr zu nehmen.

---

### *Täterkreis*

Bei beiden Delikten ist der Täter die konkret handelnde Person, hier also derjenige, der ein Abwehrsystem mit reputationsbasierenden Filtermethoden installiert und betreibt. Meist sind dies die Mitarbeiter der EDV-Abteilung des Unternehmens. Diese tun etwas Derartiges aber selten ohne entsprechende Anweisungen durch die Geschäftsführung. Die Strafbarkeit der Tat betrifft daher auch den Anstifter, denn nach § 26 StGB ist auch ein Anstifter wie ein Täter zu bestrafen. Eine Straftat im Bereich des Telekommunikationsrechts kann also ohne weiteres auch Konsequenzen für den Geschäftsführer nach sich ziehen.

Wie bereits gesehen, sind ausländische Täter nur dann vom deutschen Strafrecht erfasst, wenn Tathandlung oder Taterfolg im Inland liegen. Wird aber eine E-Mail auf einem inländischen Server unterdrückt, liegt der Taterfolg im Inland, so dass die Tat nach deutschem Strafrecht geahndet werden kann.

---

## KONSEQUENZEN FÜR DEN EINSATZ REPUTATIONSBASIERENDER FILTERMETHODEN IM UNTERNEHMEN

---

### *Vermeidung einer Strafbarkeit aus § 206 Abs. 2 Nr. 2 StGB*

Ist die Appliance so eingestellt, dass auffällige E-Mails blockiert oder sonst nicht zugestellt werden, kann dies strafrechtlich betrachtet grundsätzlich ein Problem darstellen. Da § 206 Abs. 2 Nr. 2 StGB den gesamten Fernmeldevorgang und damit neben dem Empfänger einer E-Mail auch deren Versender schützt, scheidet eine Einwilligungslösung aus praktischen Gründen aus. Zur rechtssicheren Handhabung des Filtersystems ist wiederum eine getrennte Betrachtung der Behandlung von Virus- und Spam-Mails notwendig.

Relativ unproblematisch ist die Unterdrückung virenverseuchter E-Mails. Wie bereits gesehen, gibt § 109 Abs. 1 Nr. 2 TKG dem Unternehmen die Pflicht auf, technische Schutzmaßnahmen zu ergreifen. Diese Norm wirkt sich auf den Straftatbestand rechtfertigend aus, der Verwender eines Filtersystems handelt also nicht rechtswidrig und bleibt straffrei. Die Unterdrückung von Spam-Mails ist nicht so einfach möglich. Eine Rechtfertigung nach § 109 Abs. 1 TKG ist nicht möglich, weil Spam zwar lästig ist, jedoch grundsätzlich keine Bedrohung für das Fernmeldegeheimnis oder ein Telekommunikationssystem darstellt. Zum Glück kann jedoch auch Spam bei Beachtung einiger Grundregeln ohne strafrechtliche Konsequenzen gefiltert werden.

Wie gesehen, erfolgt die Filterung bei IronPort-Appliances in zwei Stufen. In der ersten Stufe erfolgt eine SenderBase-Abfrage des Reputationswerts der IP-Adresse. Diese Abfrage findet direkt nach Mitteilung der IP-Adresse, also im Rahmen der Vorbereitung des eigentlichen Telekommunikationsvorgangs statt. Ist der Reputationswert so niedrig, dass die E-Mail nach der jeweils eingestellten Policy abgelehnt wird, lässt die Appliance die Übertragung der E-Mail in das Empfängersystem nicht zu. Zur Erfüllung des Tatbestands des § 206 StGB müsste die E-Mail jedoch bereits „anvertraut“, also in den technischen Verfügungsbereich des Servers gelangt sein. Dieser Zeitpunkt wird hier nicht erreicht, da die Appliance bereits den Versuch einer Kontaktaufnahme nicht zulässt. Eine Strafbarkeit nach § 206 StGB scheidet also auf der ersten Stufe der Überprüfung aus, obwohl die Spam-Email zuverlässig abgewehrt wurde.

Ist der Reputationswert der IP-Adresse dagegen hoch genug, wird die Übertragung der E-Mail auf das Empfängersystem zugelassen. Vertrauenswürdige E-Mails werden direkt ihren Empfängern zugestellt. Verdächtige E-Mails durchlaufen zunächst die zweite Stufe der Prüfung. Hier wird der Inhalt der E-Mail überprüft. Da die E-Mail bereits übertragen ist, gilt sie jetzt als „anvertraut“ im Sinne des § 206 Abs. 2 Nr. 2 StGB. Würde sie nun schlicht gelöscht, wäre der Straftatbestand des Unterdrückens erfüllt, da sie ihren Empfänger nicht mehr erreicht. Eine Umleitung der E-Mail in eine dem Empfänger unzugängliche Quarantäne ist aus demselben Grund nicht möglich. Durch eine entsprechende Konfiguration einer IronPort-Appliance lässt sich dieses Problem jedoch vermeiden: wird eine E-Mail als Spam erkannt, sollte das System sie in eine Quarantäne leiten, die dem Empfänger jederzeit zugänglich ist. Das System kann dann zudem periodisch Zusammenfassungen über den Inhalt des Quarantänefachs an die Nutzer senden, wobei jede E-Mail in Quarantäne über einen Link in diesen Benachrichtigungen unmittelbar zugänglich ist. Spam wird also im Hinblick auf § 206 StGB nicht „unterdrückt“, sondern lediglich „umgeleitet“, so dass der Straftatbestand wiederum nicht erfüllt ist.

---

### *Vermeidung einer Strafbarkeit aus § 303 a StGB (Datenveränderung)*

Da § 303 a StGB anders als der § 206 StGB nicht den Fernmeldevorgang an sich, sondern nur den Empfänger einer E-Mail schützt, stellen sich bei der Handhabung dieser Norm weniger Probleme, obwohl es hierbei unerheblich ist, ob das Unternehmen die private Nutzung zugelassen oder untersagt hat. Dieser Umstand ist nur im Hinblick auf mögliche Entschuldigungstatbestände relevant: für eine Rechtfertigung der Virenprüfung kann ein Unternehmen, das die private Nutzung untersagt hat, nicht auf § 109 Abs. 1 Nr. 2 TKG zurückgreifen, da diese Norm nur Diensteanbietern hilft. Ist ein Unternehmen kein Diensteanbieter, kann es sich jedoch auf einen anderen Rechtfertigungsgrund berufen. Eine virenverseuchte E-Mail stellt nämlich eine Gefahr für das Netzwerk eines Unternehmens dar. Wird sie aufgehalten und gelöscht bzw. anderweitig unschädlich gemacht, ist dies nicht rechtswidrig, da ein so genannter rechtfertigender Notstand zur Abwendung der Gefahr vorliegt.

Zur Handhabung von Spam gilt das zu § 206 Abs. 2 Nr. 2 StGB Gesagte entsprechend. Eine vollständige Unterdrückung bzw. Löschung wäre grundsätzlich rechtswidrig. Wenn entsprechende E-Mails jedoch lediglich in einen Quarantäne-Bereich umgeleitet werden und weiterhin dem Zugriff des Empfängers unterliegen, ist der Tatbestand nicht erfüllt. Darüber hinaus ist zu bedenken, dass im Rahmen des § 303 a StGB nur der Empfänger der E-Mail geschützt ist. Deswegen sollte zudem als eine weitere Rechtfertigung eine Einwilligung in die Filtermaßnahme aller potentiellen Empfänger eingeholt werden. Auch in diesem Fall ist dann bereits der Tatbestand des § 303a StGB nicht mehr erfüllt.

## 5. FREQUENTLY ASKED QUESTIONS ZUR RECHTSSICHEREN GESTALTUNG DER E-MAIL-FILTERUNG MITTELS REPUTATIONSBASIERTER FILTERSYSTEME

### IST DER EINSATZ VON REPUTATIONSFILTERUNGS-TECHNIKEN RECHTLICH UNBEDENKLICH?

Der Einsatz moderner reputationsbasierter E-Mail-Filtertechnologien ist so lange unbedenklich, wie die Konfiguration dieser Systeme die im jeweiligen Einzelfall geltenden Rechtsbestimmungen berücksichtigt. Dazu ist immer eine Abwägung im Einzelfall erforderlich, da nicht für jeden Nutzer dieselben Regeln gelten.

### WIE MÜSSEN DIE SYSTEME AUFGESETZT WERDEN, UM DATENSCHUTZRECHTLICH KONFORM ZU SEIN?

Die datenschutzrechtliche Konformität hängt schlicht davon ab, ob die Filter personenbezogene Daten verarbeiten. Dies ist immer dann nicht der Fall, wenn eine protokolldaten-gestützte Vorfilterung stattfindet, bei der die Informationen über die IP-Adresse des Sendernetzwerkes nicht aus der bereits übermittelten E-Mail gewonnen werden, sondern bereits im Vorfeld beim ersten Versuch einer Kontaktaufnahme des Sendersystems ausgewertet werden. Wird ein derartiger Verbindungsversuch aufgrund eines schlechten Reputationswertes zurückgewiesen, ist dies datenschutzrechtlich unbedenklich.

Bei der darüber hinaus stattfindenden Überprüfung der E-Mail gelten dieselben Maßstäbe wie beim Einsatz herkömmlicher Spam-Filter: eine Filterung von E-Mails zur Vermeidung negativer Konsequenzen für das Unternehmen, die nicht händisch, sondern automatisiert stattfindet, ist datenschutzrechtlich auch ohne eine Einwilligungserklärung jedes einzelnen Betroffenen zu rechtfertigen. Eine zusätzliche Einwilligung zumindest der eigenen Mitarbeiter ist jedoch dennoch sinnvoll, um die rechtlichen Risiken weiter zu verringern.

### WAS HAT DAS FERNMELDEGEHEIMNIS MIT SPAM-FILTERUNG ZU TUN?

Das grundgesetzlich geschützte Fernmeldegeheimnis trifft jeden Telekommunikationsanbieter und beschränkt in einem erheblichen Maße die Möglichkeiten, übertragene E-Mails zu filtern und auf unerwünschte Inhalte hin zu überprüfen. Außer den Internet-Providern, die automatisch dem Telekommunikationsgesetz (TKG) unterliegen, gilt dies jedoch auch für solche Unternehmen, die ihren Mitarbeitern die private Nutzung der E-Mail-Systeme ausdrücklich erlauben oder die zumindest stillschweigend dulden.

Angesichts einer Strafbarkeit aus § 206 StGB sind Verletzungen des Fernmeldegeheimnisses auch keine Kavaliersdelikte, sondern ein ernst zu nehmender Aspekt des rechtskonformen Einsatzes von E-Mail-Filtern.

### MACHT MAN SICH DURCH DEN EINSATZ VON E-MAIL-FILTERN STRAFBAR?

Abgesehen von § 206 StGB gibt es noch weitere Strafrechtstatbestände, die einen unüberlegten Einsatz von E-Mail-Filtern durchaus riskant werden lassen können. Hierzu gehören in erster Linie die Tatbestände der Datenveränderung (§ 303a StGB). Durch Einwilligungserklärungen und eine geeignete Konfiguration lassen sich auch hierbei die strafrechtlichen Risiken minimieren oder sogar ganz ausschalten.

## WAS BEWIRKT EINE EINWILLIGUNG DER MITARBEITER IN DIE FILTERUNG?

§ 88 TKG, der den Schutz des Fernmeldegeheimnisses regelt, ist dispositiv, also abbedingbar. Eine Einwilligung der Mitarbeiter in die Kenntnisnahme und Verarbeitung ihrer Emails ist daher möglich und stellt eine rechtssichere Gestaltungsmöglichkeit zur Verhinderung einer Strafbarkeit aus § 206 StGB dar. Der Tatbestand des § 303a StGB ist ebenfalls dann nicht verwirklicht, wenn ein Einverständnis der Beteiligten vorliegt.

Datenschutzrechtlich kann argumentiert werden, dass eine Prüfung von eingehenden Emails ausschließlich zur Erkennen von Spam-E-Mails und dessen deren Umleiten in einen Quarantäne-Ordner durch eine vollautomatische Sortierung ohne Zugriffsmöglichkeit des Unternehmens sich im Rahmen der berechtigten Interessen des Unternehmens bewegt und damit zulässig ist. Da die Kontrollmöglichkeiten des Unternehmens jedoch im Einzelnen noch nicht abschließend rechtlich geklärt sind, ist die Einholung einer Einwilligung der Mitarbeiter und der ansonsten Betroffenen eine rechtssichere Möglichkeit zur Vermeidung datenschutzrechtlicher Sanktionen.

*NÖRR STIEFENHOFER LUTZ wird vom unabhängigen Fachmagazin JUVE regelmäßig zu einer der führenden deutschen Wirtschaftskanzleien für IT-Recht gekürt. Mit Büros in München, Berlin, Frankfurt, Dresden und Düsseldorf sowie in vielen mittel- und osteuropäischen Staaten berät sie Unternehmen insbesondere bei der effizienten und zugleich wirtschaftlichen Umsetzung von gesetzlichen und regulatorischen IT-Compliance-Anforderungen. Nähere Informationen sind unter [www.noerr.com](http://www.noerr.com) abrufbar.*

*Der Autor, Dr. Jyn Schultze-Melling LL.M., hat sich auf das Thema IT-Compliance spezialisiert und berät vom Münchener Büro aus große Mittelständler und Großunternehmen insbesondere in allen Fragen des Datenschutzes und des IT-Sicherheitsrechts. Zudem vermittelt er als Publizist, regelmäßiger Referent auf Veranstaltungen und gefragter Dozent bei Seminaren und Fortbildungen spezifisches Praxis-Know-how zur IT-Compliance.*

*Dieses Whitepaper stellt einen rechtlichen Überblick dar und ersetzt nicht die rechtliche Beratung im Einzelfall. Es wird daher um Verständnis dafür gebeten, dass für die Richtigkeit und Vollständigkeit der in diesem Whitepaper enthaltenen Angaben und Ausführungen trotz der Versicherung sorgfältiger Recherche keine Haftung übernommen werden kann. Im Falle rechtlicher Fragen zu diesem Whitepaper steht Ihnen der Autor gerne unter der E-Mail-Adresse [jyn.schultze-melling@noerr.com](mailto:jyn.schultze-melling@noerr.com) zur Verfügung.*

*Für technische Rückfragen und Anregungen wenden Sie sich bitte an: IronPort Systems GmbH, Angelika Felsch, Marketing Manager Central & Eastern Europe, Tel.: +49 (0)89/45 22 27-14, E-Mail: [afelsch@IronPort.com](mailto:afelsch@IronPort.com).*