

## **Elektronische Post und Datenschutz**

[Elektronische Post unterliegt dem Fernmeldegeheimnis](#)

[Das Mitlesen von elektronischer Post kann nur durch Verschlüsselung verhindert werden](#)

[Elektronische Post kann gefährliche Trojanische Pferde enthalten](#)

### **Elektronische Post unterliegt dem Fernmeldegeheimnis**

Elektronische Post ist sowohl als Telekommunikationsdienst als auch als Teledienst zu bewerten. Damit sind nicht nur das Bundesdatenschutzgesetz (BDSG) und Landesdatenschutzgesetze wie das Bremische Datenschutzgesetz (BrDSG) einschlägig, sondern auch das Teledienstedatenschutzgesetz (TDDSG) und das Telekommunikationsgesetz (TKG). Das TDDSG und das TKG – insbesondere § 85 über das Fernmeldegeheimnis und § 89 über Datenschutz – gelten allerdings nur, wenn der Telekommunikationsdienst Dritten zur Verfügung gestellt wird. Dritte im Sinne des TKG sind nicht nur Behörden und Unternehmen, für die elektronische Post weitergeleitet und in Postfächern gespeichert wird. Dritte sind aber auch solche Mitarbeiter, die den Dienst der elektronischen Post für private Zwecke nutzen bzw. bei denen die private Nutzung vom Arbeitgeber geduldet wird.

Individuelle Postfächer, die sowohl dienstlich als auch privat genutzt werden, unterliegen demnach dem Fernmeldegeheimnis gemäß § 85 TKG. Die Anwendbarkeit des TKG, das den Inhalt der elektronischen Post unter das grundrechtlich geschützte Fernmeldegeheimnis unterstellt, hat zur Folge, dass individuelle Postfächer nicht von den für den Mail-Server zuständigen Administratoren eingesehen werden dürfen. Auch dürfen keine fehlgeleiteten, persönlich adressierten Mails geöffnet werden, um anhand des Inhalts den korrekten Absender zu ermitteln.

Sowohl privat als auch dienstlich genutzte elektronische Postfächer erfordern daher restriktive Vertretungs- und Abwesenheitsregelungen. Um das Fernmeldegeheimnis zu wahren, sollten daher ohne Zustimmung des Betroffenen keine Mails an andere E-Mail-Adressen weitergeleitet werden. Und auch mit Zustimmung des Betroffenen ist eine Weiterleitung problematisch, da hiervon ebenso der Absender der Nachricht betroffen ist.

### **Das Mitlesen von elektronischer Post kann nur durch Verschlüsselung verhindert werden**

Elektronische Post wird auf dem Weg durch das Internet von zahlreichen Rechnern weitergeleitet, bis sie bei ihrem eigentlichen Empfänger ankommt. Jeder, der Zugang zu diesen Netzwerkrechnern hat, kann die Nachricht mitlesen, ohne dass Absender und Empfänger dies bemerken. Der Absender kennt meistens noch nicht einmal den Weg, den die Nachricht zum Empfänger überhaupt nimmt.

Es kann davon ausgegangen werden, dass ein Großteil des Internet-Datenverkehrs automatisiert überwacht und nach Schlüsselbegriffen

ausgewertet wird. Um zu verhindern, dass sensible persönliche oder geschäftliche Informationen beim Transport über das Internet von Außenstehenden mitgelesen werden, sollten die Nachrichten beim Absender vorab verschlüsselt und beim Empfänger wieder entschlüsselt werden.

Zur Verschlüsselung von elektronischer Post eignen sich besonders sogenannte asymmetrische Verschlüsselungsverfahren wie beispielsweise PGP (Pretty Good Privacy). PGP ist im Internet mittlerweile zu einem De-facto-Standard geworden und als Freeware frei verfügbar, sofern es nicht kommerziell eingesetzt wird. PGP, das 1991 von dem US-Amerikaner Phil Zimmermann entwickelt wurde, können Sie von zahlreichen Web-Servern laden:

<http://www.pgpi.com/>  
[www.cert.dfn.de/team/pubkeys.html](http://www.cert.dfn.de/team/pubkeys.html)  
[www.heise.de/ct/pgpCA/download.shtml](http://www.heise.de/ct/pgpCA/download.shtml)

Hierbei generiert jeder E-Mail-Anwender einmalig ein Schlüsselpaar, bestehend aus einem öffentlichen und einem geheimen Schlüssel. Ein derartiges Verfahren nennt sich asymmetrisch, da elektronische Post, die mit dem öffentlichen Schlüssel codiert wurde, nur noch mit dem geheimen Schlüssel entschlüsselt werden kann. Um elektronische Post verschlüsselt versenden zu können, muss daher dem Absender der öffentliche Schlüssel des Empfängers bekannt sein. Umgekehrt kann mit Hilfe des eigenen geheimen Schlüssels elektronische Post auch so digital signiert werden, dass mit dem öffentlichen Schlüssel geprüft werden kann, ob die Nachricht tatsächlich vom Empfänger stammt und ob sie auf dem Weg durch das Internet verändert wurde.

Auch dem Landesbeauftragten für den Datenschutz der Freien Hansestadt Bremen können Mails geschickt werden, die per PGP verschlüsselt wurden. [Unseren öffentlichen Schlüssel können Sie an dieser Stelle herunterladen.](#)

## **Elektronische Post kann gefährliche Trojanische Pferde enthalten**

Ein zunehmendes Problem stellen Viren und Trojanische Pferde dar, die entweder als Anlage oder – angesichts HTML-fähiger Client-Software – als direkter Bestandteil einer Mail verschickt und lokal auf dem Internet-PC zur Ausführung gelangen können.

Da im Internet Werkzeuge verfügbar sind, die die Entwicklung von Viren vereinfachen bzw. das Muster von Viren entscheidend verändern, kann auf die Wirksamkeit von Virensclannern allein nicht mehr vertraut werden. Einerseits besteht die Gefahr, dass die Trojanischen Pferde über den Mail-Server selbstständig Daten aus dem lokalen Netz heraus an beliebige Internetadressen versenden, ohne dass es der Benutzer bemerken würde. Andererseits können Trojanische Pferde wie beispielsweise Back Orifice oder NetBus Server-Funktionen enthalten, die von anderen Netzanwendern aufgerufen und zur Fernsteuerung des jeweiligen PC genutzt werden.

Diese Risiken können auch durch den Einsatz einer Firewall nicht wirksam unterbunden werden, da Trojanische Pferde in einer rechtmäßigen Umgebung aufgerufen werden und sich von anderen Anwendungsfunktionen technisch kaum unterscheiden lassen. Über den

Einsatz von aktuellen Virenscannern hinaus ist es daher erforderlich, den potentiellen Zugriff auf sensible personenbezogene Daten aus dem Internet heraus von vornherein drastisch einzuschränken.

Wer darauf nicht verzichten möchte, sollte zumindest eine der folgenden Sicherheitsmaßnahmen treffen:

- **Getrennte Arbeitsumgebungen:**  
Auf dem Internet-PC werden zwei Arbeitsumgebungen eingerichtet. In der Produktionsumgebung wird auf sensible Daten zugegriffen, während die Internetumgebung ausschließlich für den Internetzugang einschließlich elektronischer Post zur Verfügung steht. Die beiden Umgebungen werden entweder auf zwei verschiedene Benutzerkennungen abgebildet, denen verschiedene Rechte zugeordnet sind, oder auf zwei getrennte Betriebssysteme. Der Anwender wechselt je nach Erforderlichkeit zwischen den beiden Umgebungen, indem er sich entweder beim Betriebssystem ab- und wieder anmeldet oder das gesamte System neu startet.
- **Einsatz von Terminal-Servern:**  
Sämtliche sicherheitskritischen Internetdienste werden auf einem Terminal-Server ausgeführt, so dass Webseiten oder Inhalte von elektronischer Post lediglich in Form einer Grafik vom Terminal-Server an die jeweiligen PC übertragen werden. Da der Terminal-Server die eigentliche Datenverarbeitung übernimmt, können auch keine unerwünschten Fehlfunktionen auf dem Rechner zur Ausführung gelangen, auf dem ansonsten sensible Daten verfügbar sind. Um im Falle einer erfolgreichen Internetattacke auf den Terminal-Server zu verhindern, dass der Angreifer auch auf andere Rechner zugreifen kann, sollte die Verbindung zwischen Terminal-Server und dem zu schützenden lokalen Netz möglichst durch eine Firewall kontrolliert werden.
- **Laufzeitüberwachung von Programmen:**  
Per elektronischer Post oder über das Internet übertragene Programme werden einer Laufzeitüberwachung – mit der Java-Sandbox vergleichbar – unterstellt. Die Laufzeitüberwachung kann sich auch auf bestimmte sensible Dateien beziehen, die auf der Festplatte gespeichert werden.