Zum Umgang mit E-Mail-Accounts von abwesenden oder nicht ansprechbaren Mitarbeitern/Mitarbeiterinnen

Problemstellung: Zahlreiche Geschäftsprozesse an der Hochschule werden inzwischen per E-Mail abgewickelt, wie beispielsweise die Anmeldung zu Vortragsveranstaltungen oder die Terminabsprache zu Vorstellungsgesprächen. Doch was passiert, wenn der/die Inhaber/in des entsprechenden Mitarbeiter-Accounts nicht anwesend oder nicht mehr ansprechbar ist und keine andere Person die Zugangsdaten kennt? Dürfen sich Vorgesetzte oder Mitarbeiter/innen Zugriff auf die E-Mails verschaffen? Darf ohne Wissen des Inhabers/der Inhaberin eine automatische Abwesenheitsmeldung für seine/ihre E-Mail-Adresse eingerichtet werden? Für die Beantwortung dieser Fragen sind vor allem das Fernmeldegeheimnis, der Datenschutz, strafrechtliche Normen sowie das Persönlichkeitsrecht zu beachten. Aber gerade an dienstlichen E-Mails kann ein berechtigtes Interesse (privat oder geschäftlich) des Vorgesetzten oder anderer Personen bestehen. Es kann aber auch im Interesse des Mitarbeiters/der Mitarbeiterin selbst liegen, dass Dritte die E-Mails einsehen können, etwa wenn Geschäfte weitergeführt oder Termine verwaltet werden müssen.

Handlungsempfehlung:

1. Zugriffsverschaffung auf die E-Mails

Auch wenn es technisch relativ einfach möglich wäre, die Mailbox des entsprechenden abwesenden Mitarbeiters/der entsprechenden Mitarbeiterin „zu knacken“, sind doch erhebliche juristische Hürden zu beachten, deren Missachtung schwerwiegende (auch strafrechtliche) Konsequenzen zur Folge hat.

Wurden die E-Mails schon abgerufen und befinden sich auf dem Rechner des Mitarbeiters/der Mitarbeiterin, (z.B bei Nutzung des POP-Dienstes des Rechenzentrums), ist der Übermittlungsvorgang abgeschlossen und es darf unter bestimmten Voraussetzungen Zugriff verschafft werden.

Das Fernmeldegeheimnis gilt über §§ 3 Nr. 6 und Nr. 10, 88 Abs. 2 Telekommunika-tionsgesetz – TKG sowohl für private als auch für staatliche Anbieter von Telekom-munikationsdiensten. Da die Universität bzw. das Rechenzentrum die private Nut-zung erlaubt oder duldet, ist sie bzw. es in diesem Sinne Diensteanbieter und hat somit das Fernmeldegeheimnis zu beachten. Das Fernmeldegeheimnis schützt allerdings nur die näheren Umstände der Übermittlung und die Kommunikationsinhalte während des Übermittlungsvorgangs. Der Inhalt ist nach Abschluss der Übermittlung nicht mehr geschützt (vgl. auch Urteil des Bundesverfassungsgerichts vom 02.03.2006, Az. 2 BvR 2099/04). Das Fernmeldegeheimnis wird hier also nicht berührt und steht damit einer Zugriffsverschaffung nicht entgegen.

Dies gilt allerdings nur für dienstliche E-Mails, deren Kenntnis zwingend erforderlich ist, um die Aufgaben der Universität fortzuführen (z.B. Durchführung von Lehrveranstaltungen, Prüfungen etc.). Dabei ist das Interesse der Hochschule mit dem des Mitarbeiters/der Mitarbeiterin abzuwägen.

Um Interessenskollisionen zu vermeiden, sollte daher ein Datenschutzbeauftrag-ter/eine Datenschutzbeauftragte die Daten sichten und in dienstlich erforderliche und persönlichkeitsrelevante E-Mails einordnen.

Liegen die E-Mails hingegen noch auf einem zentralen Server, ist davon auszugehen (Die Rechtslage

ist hier noch nicht geklärt – das trifft somit auch den IMAP-Dienst des Rechenzentrums), dass sie dem Fernmeldegeheimnis (Art. 10 Abs. 1 Grundgesetz - GG) unterliegen und ein Zugriff nur unter dessen strengen Voraussetzungen zulässig ist. Das gilt insbesondere, wenn die E-Mails noch ungelesen sind, da der Übermittlungsvorgang erst beendet ist, wenn die E-Mails tatsächlich im alleinigen Machtbereich des Empfängers/der Empfängerin angelangt sind und die Gefahr des Eindringens in den Kommunikationsvorgang nicht mehr besteht.
(http://www.dfn.de/rechtimdfn/empfehlungen/handlungsempfehlungen/abwehrspam0/)

In diesem Fall ist daher auch die Einsichtnahme durch unbeteiligte Dritte (wie ei-nem/einer Datenschutzbeauftragten) zum Zwecke der Vorsortierung juristisch gese-hen ausgesprochen heikel.

2. Schalten einer automatischen Abwesenheitsnotiz

Damit wenigstens die zukünftige Korrespondenz nicht mehr auf die fragliche E-Mail-Adresse aufläuft, kann über die erzwungene Schaltung einer automatischen Abwesenheitsnotiz nachgedacht werden. Die Einrichtung einer Abwesenheitsnotiz ist nämlich deutlich weniger belastend und eingriffsintensiv und daher eher zulässig als eine Einsichtnahme in die Nachrichten. Zum einen werden die eingehenden Nachrichten angenommen und dem Empfänger/der Empfängerin in seinem/ihrem Postfach zur Verfügung gestellt. Es findet also keine Abweisung der ankommenden E-Mails statt. Zum anderen werden die E-Mails nicht an andere Mitarbeiter/innen weitergeleitet, was im Hinblick auf das Fernmeldegeheimnis und den Datenschutz problematisch sein kann, da bei einer Weiterleitung und erlaubter/geduldeter Privatnutzung unter Umständen auch private Mails dem Vertreter zur Verfügung gestellt würden. Bei einer Abwesenheitsnotiz sollte deutlich gemacht werden, dass es sich um eine automatisierte Antwort des Servers bzw. des Providers handelt und nicht um eine Nachricht des/der nicht erreichbaren Empfängers/Empfängerin. Zudem sollte klargestellt werden, dass eine Weiterleitung nicht erfolgt und deshalb bei dringenden Angelegenheiten ein/e Vertreter/in, dessen/deren Adresse genannt werden sollte, kontaktiert werden kann. Keinesfalls darf der Grund für die Abwesenheit oder eine Dauer genannt werden, da dies für den zu erfüllenden Zweck (Aufrechterhaltung des Betriebs, Organisation) nicht erforderlich ist und daher das Persönlichkeitsrecht des/der Betroffenen verletzen würde. Wenn möglich, ist der/die Inhaber/in des Accounts zu informieren und sein/ihr Einverständnis einzuholen. Es könnte sogar eine Pflicht zur Einwilligung bestehen, die sich entweder aus dem Nutzungs- oder Dienstverhältnis ausdrücklich ergibt oder aber eine Nebenpflicht darstellt. Auch kann bei einer so wenig benachteiligenden Maßnahme wie einer automatischen Abwesenheitsnotiz das Einverständnis in aller Regel vermutet werden. Eine solche Vermutung ist aber nur zulässig, wenn eine ausdrückliche Einwilligung nicht eingeholt werden kann, da der/die Betroffene nicht erreichbar ist. Kann man hingegen bei ihm/ihr nachfragen, geht dies vor. (DFN, Hannes Obex)

3. Vorsorge ist besser als Nachsorge

All diese Schwierigkeiten lassen sich durch organisatorische Vorsichtsmaßnahmen vermeiden.

a) Klären Sie, ob die Mitarbeiter/innen entweder bereit sind, ihre Passwörter für Not-fälle an einem sicheren Ort zu deponieren und im Bedarfsfall der/die Vorgesetzte darauf zugreifen darf oder bereit sind, die Passwörter vertrauten Kolleginnen und Kollegen mitzuteilen, welche dann im Bedarfsfall die Mailbox öffnen dürfen. Auf diese Weise ist das Einverständnis für das Vorgehen in Notfällen im Vorfeld gesi-chert und im tatsächlichen Schadensfall kann sofort gehandelt werden.

b) Richten Sie für dienstliche Notwendigkeiten sogenannte funktionale E-Mail-Adressen ein, beispielsweise sekretariat@lehrstuhl.uni-freiburg.de und regeln Sie intern mit allen, die Zugriff auf diese Mailbox erhalten, dass nur dienstliche Korrespondenz darüber abgewickelt werden darf. Bei solchen Mailboxen können Sie eine Notfallregelung für Passwörter erwarten bzw. fordern. Aufgrund

der Na-menswahl ist allen Beteiligten klar – insbesondere auch den Absendern von E-Mails –, dass solche Mailadressen nicht für persönliche Kommunikation genutzt werden dürfen.

Hinweis: Zu diesem Thema hat das Rechenzentrum ein Beispielformular erstellt.

E-Mail - Artikelübersicht