Recht und Datenschutz

private E-Mails an der Hochschule

Eine Ausarbeitung von Gruppe 4:

Maxim Bergmann 7006347
Victor Ginsheimer 7006705

Betreuer:

Prof.Dr. Schiemann-Lillie

Inhaltsverzeichnis

1. Gesetzlicher Rahmen **2**
1.1 Telekommunikationsgesetz 2
1.2 Telemediengesetz 2

2. Anforderungen **3**
2.1 Datenvermeidung und Datensparsamkeit 3
2.2 Transparenz 3
2.3 Verletzung des Schutzes 3
2.4 Vertraulichkeit und Integrität 4
2.5 Spam und Viren 4

3. Arbeitsverhältnis **5**
3.1 Beginn - Vereinbarung 5
3.2 Ende - Aufbewahrung 6

4. Beispiel - Umsetzung **6**
4.1 Konzept 6
4.2 Schwierigkeiten 7

5. Quellen **8**

1. Gesetzlicher Rahmen

Sollte die Hochschule die Nutzung von Internetdiensten, darunter auch E-Mails, den Mitarbeitern gestatten, so muss sie die geltenden Gesetzgebungen berücksichtigen.
Für den Fall, dass es sich dabei um rein geschäftliche Anwendungen handelt, gilt das Bundesdatenschutzgesetz, bzw. das Niedersächsische Datenschutzgesetz. In unserem Fallbeispiel geht es jedoch um die Nutzung von privaten E-Mails innerhalb der Hochschule; hier treten das Telekommunikationsgesetz (TKG) und das Telemediengesetz (TMG) in Kraft.

1.1 Telekommunikationsgesetz

Dienstanbieter § 3 Nr.6 TKG:
jeder, der ganz oder teilweise geschäftsmäßig

a) Telekommunikationsdienste erbringt oder
b) an der Erbringung solcher Dienste mitwirkt

Laut § 88 TKG ist es der Hochschule nicht gestattet, die Inhalte der privaten E-Mails einzusehen (Fernmeldegeheimnis), darf diese jedoch zu Abrechnungszwecken speichern.
Gemäß § 113a Abs.1 TKG unterliegt die Hochschule jedoch nicht der Pflicht/Möglichkeit die Verkehrsdaten zu speichern. Also bspw. Zuordnung Arbeitsplatz zu IP-Adressen etc.
Das Fernmeldegeheimnis besteht auch nach Beendigung des Arbeitsverhältnisses zwischen Hochschule und Mitarbeiter.

1.2 Telemediengesetz

§ 2 Abs.1 TMG ordnet die Hochschule als Diensteanbieter ein. Während das TKG sich im Wesentlichen auf den Transfer der Daten konzentriert, regelt das TMG die Rechte für die Inhalte an sich. Und sagt aus, dass die Hochschule personenbezogene Daten (E-Mails) nur dann verwenden darf, falls es der Rechtsverfolgung dient. Ansonsten überschneiden sich TMG und TKG in ihren Regelungen bezogen auf unseren Fall.

2. Anforderungen

2.1 Datenvermeidung und Datensparsamkeit

§ 3a BDSG (gilt in unserem Beispiel nicht direkt, ist aber dennoch eine starke Richtlinie) besagt, dass man bei der Datenverarbeitung so wenig wie möglich personenbezogene Daten aufwenden/ansammeln soll. Das heißt z. B. Emails sollten wenn, dann nur auf einem Server + max. 1 Mirror-Server (für Backups) gespeichert werden und keine Kopie auf den lokalen Arbeitsplätzen angelegt werden. Am besten sollten die E-Mails auch anonymisiert abgelegt werden, so dass nur eine Zuordnung der E-Mail zum Sender/Empfänger besteht, wenn dieser diese abruft oder versenden will (also eingeloggt ist).

2.2 Transparenz

§ 93 TKG
Die Angestellten der Hochschule müssen auch ebenfalls über technische Maßnahmen informiert werden, damit sie wissen wie welche Datenschutzmaßnahmen ergriffen werden.

2.3 Verletzung des Schutzes

Sollten die Maßnahmen, die zur Sicherung der personenbezogenen Daten gefährdet werden, also wenn z. B. festgestellt wird, dass der Verschlüsselungsalgorithmus für den E-Mail-Transfer nicht mehr den Sicherheitsstandards entspricht, müssen die betroffenen Mitarbeiter, sowie die Bundesnetzagentur und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, unverzüglich informiert werden.

§ 109a TKG (2)
Die Benachrichtigung an die Betroffenen muss mindestens enthalten:

1. die Art der Verletzung des Schutzes personenbezogener Daten,
2. Angaben zu den Kontaktstellen, bei denen weitere Informationen erhältlich sind, und
3. Empfehlungen zu Maßnahmen, die mögliche nachteilige Auswirkungen der Verletzung des Schutzes personenbezogener Daten begrenzen.

§ 109a TKG (3)
Die Hochschule hat ein Verzeichnis der Verletzungen des Schutzes personenbezogener Daten zu führen, das Angaben zu Folgendem enthält:

1. zu den Umständen der Verletzungen,
2. zu den Auswirkungen der Verletzungen und
3. zu den ergriffenen Abhilfemaßnahmen.

2.4 Vertraulichkeit und Integrität

Es muss sichergestellt sein, dass jede Übertragung von E-Mails, egal von welchem Gerät, sicher abgehandelt werden soll. Somit muss auch auf Smartphones, Tablets, Laptops der Mitarbeiter eine Verschlüsselung stattfinden. So kann sichergestellt werden, dass auch innerhalb des Unternehmens kein Dritter den Datenverkehr mitschneiden kann.

2.5 Spam und Viren

Wie dem Abschnitt 1.1 zu entnehmen ist, darf die Hochschule die privaten E-Mails nicht ansehen, da diese dem Fernmeldegeheimnis unterliegen. Doch muss sich die Schule auch vor Viren schützen können und den Mitarbeitern sollte natürlich auch Schutz vor Spam Nachrichten gewährleistet werden. Das geht nicht ohne Filterung und das erfordert nun doch eine Form von Inhaltsprüfung. Dabei muss man darauf achten, dass so wenig wie möglich personenbezogene Daten überprüft werden.

Beispiel: Es ist in Ordnung den Nachrichten-Header auszulesen auf: E-Mail Protokoll, Protokoll-Version, Dateityp der Anhänge (insbesondere ausführbare Dateien), etc.
Hat die Hochschule eine IP-Blacklist, z. B. weiß man, dass Verbindungen von bestimmten IP-Adressen im Netz, als schädlich eingestuft wurden, laut BSI[1] oder Empfehlungen von Sicherheitsfirmen oder Statistiken, dann muss auch der IP-Header des E-Mail-Verkehrs geprüft werden. Dabei kann man aber auch schon oft den Empfänger feststellen, was wiederum deutlich macht, dass IP-Adressen ein personenbezogenes Datum darstellen. Der Betroffene Mitarbeiter der Hochschule muss somit darüber informiert werden, dass eine IP-Blacklist verwendet wird, und er/sie muss seine/ihre Zustimmung freiwillig erteilen.

Das BSI hat zudem auch einen großen Katalog an Strategien für Unternehmen und Organisationen um gegen unerwünschte E-Mails vorzugehen:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Antispam/Antispam-Strategien.html
Nicht alle davon sind aber mit dem Datenschutz zu vereinbaren und sollten somit vorab genau in dieser Hinsicht geprüft werden, bevor sie dann an der Hochschule eingesetzt werden.

3. Arbeitsverhältnis

3.1 Beginn - Vereinbarung

Damit man als Mitarbeiter der Hochschule weiß, dass alle Anforderungen aus Abschnitt 2 getroffen werden, und damit man, sollte eine Rechtsverletzung durch die Hochschule eintreten, auch sicher rechtliche Maßnahmen ergreifen kann, ist im Vorab mit der Hochschule eine besondere Dienstvereinbarung zu E-Mail und Internet am Arbeitsplatz zu treffen.

[1] Bundesamt für Sicherheit in der Informationstechnik

Diese Dienstvereinbarung[2] enthält und gliedert sich im wesentlichen wie folgt:

1. Geltungsbereich und Zweckbestimmung
2. Organisatorische Grundsätze
3. Zulässigkeit der Nutzung
4. Verhaltensgrundsätze
5. Information und Schulung der Beschäftigten
6. Verantwortlichkeit
7. Protokollierung und Kontrolle
8. Maßnahmen bei Verstößen / Missbrauchsregelung
9. Grundsätze für eine Nutzung behörden- / unternehmensfremder Kommunikationssysteme
10. Änderungen und Erweiterungen
11. Inkrafttreten

3.2 Ende - Aufbewahrung

Während die geschäftlichen E-Mails Eigentum der Hochschule sind und somit jederzeit von der Hochschule eingesehen werden dürfen, gilt dies auch für den Fall, wenn das Arbeitsverhältnis zu dem Mitarbeiter endet. Bei privaten E-Mails ist das jedoch anders. Die Hochschule muss die Daten des Mitarbeiters mit Ablauf des auf die Beendigung folgenden Kalenderjahres löschen § 95 TKG (3). Und darf diese selbstverständlich bis zur Löschung nach wie vor nicht einsehen.

4. Beispiel - Umsetzung

4.1 Konzept

Die Hochschule gestattet private E-Mails. Bietet dafür aber keinen eigenen Dienst an, sondern ermöglicht nur den Zugriff auf das Webportal des Privatanbieters des Mitarbeiters (bspw. GMX, GMAIL, etc.). Dadurch erfolgt keine Speicherung personenbezogenen Daten auf den Servern der Hochschule. Gemäß Abschnitt 3.1 ist

[2] https://www.datenschutz-wiki.de/Dienstvereinbarung_E-Mail_und_Internet_am_Arbeitsplatz

dann mit jedem Mitarbeiter, dem dieser Zugang gewährt werden soll, eine Vereinbarung zu treffen. Entweder man setzt eine Vereinbarung pro Mitarbeiter auf oder formuliert Vereinbarungen für Mitarbeiter-Gruppen (Professoren, WiMi, etc.) und klärt diese darüber auf und lässt sie unterschreiben.
Als Nächstes ist sicherzustellen, dass die Mitarbeiter, sollten sie ihre privaten E-Mails bspw. vom Dienst-PC über das Firmennetz abrufen, insbesondere der Zugang zu dem Webportal verschlüsselt erfolgt (z. B. SSL). Sodass die Hochschule keine Möglichkeit hat, auch firmenintern Nachrichteninhalte, einzusehen.

4.2 Schwierigkeiten

Es gibt ein wesentliches Problem mit der Umsetzung nach dem Konzept in 4.1:
Sicherheit vor Spam und Viren.
Dadurch, dass der Mitarbeiter seine E-Mails ungefiltert und unüberwacht über das Webportal aufrufen kann, kann er auch z. B. eine ausführbare Datei empfangen und ausführen. Und das könnte dann das gesamte Firmennetz infiltrieren. Somit muss auf der Client-Seite (Dienst-PC, Dienst-Smartphone, etc.) eine Software bzw. ein Browser-Addon installiert werden, dass heuristisch überprüft, ob die Dateien die im Browser geöffnet/heruntergeladen werden, sicher sind oder nicht. Je nach Heuristik muss natürlich auch darauf geachtet werden, dass personenbezogene Daten nicht eingesehen werden, somit z. B. nur auf Informationen wie Dateitypen (*.exe, *.swf, etc.) geprüft wird.

Der Vorteil in diesem Konzept, die Hochschule muss keine Spam, Viren in Emails auf eigenen E-Mail-Servern bezüglich privater E-Mails prüfen, ist somit nicht mehr da. Den diese Prüfung muss nun auf den Clients erfolgen.

5. Quellen

https://www.datenschutz-wiki.de/E-Mail_und_Internet_am_Arbeitsplatz
05.06.2017

https://www.datenschutz-wiki.de/Transparenz
05.06.2017

https://www.datenschutz-wiki.de/Datenvermeidung_und_Datensparsamkeit
05.06.2017

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Antispam/Antispam-Strategien.html
05.06.2017

https://www.datenschutz-wiki.de/Dienstvereinbarung_E-Mail_und_Internet_am_Arbeitsplatz
05.06.2017

http://www.businessinsider.com/companies-find-loopholes-in-reading-private-emails-2013-7?IR=T
05.06.2017