Universität Bielefeld

Rektorat
Der Rektor

Dezernat IT/Orga

IT-Sicherheitsbeauftragter
Michael Sundermeyer
Telefon: 106-3032
E-Mail: michael.sundermeyer@uni-bielefeld.de
Raum-Nr.: K3-128
Az.: Bielefeld, 23.10.2013

Verteiler:

Dekan(in) der Fakultät für	Leiter(in)/Geschäftsführer(in)/Vorsitzende(r)	
Biologie Chemie Erziehungswissenschaft einschließlich WE Laborschule WE Oberstufenkolleg Geschichtswissenschaft, Philosophie und Theologie Gesundheitswissenschaften Linguistik und Literaturwissenschaft Mathematik Physik Psychologie und Sportwissenschaft einschl. Betriebseinheit Hochschulsport Rechtswissenschaft Soziologie Technische Fakultät Wirtschaftswissenschaften	Ästhetisches Zentrum BGHS BiSEd CeBiTec CITEC CoR-Lab Fachsprachenzentrum FSPM² IMW Institut für interdisziplinäre Konflikt- und Gewaltforschung Institut für Wissenschafts- und Technikforschung Interdisziplinäres Zentrum für Frauen- und Geschlechterforschung Kontaktstelle Wissenschaftliche Weiterbildung SFB 673 LiLi SFB 701 Mathematik SFB 882 Soziologie Zentrum für interdisziplinäre Forschung	Studierendenvertretung (ASTA) Vertretung der Wiss. Mitarb. Gleichstellungsbeauftragte Personalrat Personalrat der wiss. Mitarb. Schwerbehindertenvertretung Hochschulrechenzentrum Universitätsbibliothek CIO IT Referat für Kommunikation Rektor, Prorektoren, Kanzler, Ständige Vertreterin des Kanzlers, Referent des Rektors SL_K5 Zentrale Universitätsverwaltung: Dez. I, Dez. II, Abt. II.1, II.2, II.3 Dez. III, Abt. III.1, III.2, III.3, III.4 Dez. F, Abt. F.1, F.2, F.3 Dez. FM, Abt. FM.1, FM.2, FM.3, FM.4, FM.5, FM.6 Dez. FFT, Abt. FFT.1 Dez. IT/Orga, Abt. IT/Orga.1, Abt. IT/Orga.2 Abt. Z.1 Justitiariat

Vertraulichkeit und Sicherheit von Forschungsdaten

Aus aktuellem Anlass wird darauf hingewiesen, dass eine Verarbeitung von Forschungsdaten außerhalb der Universität mit erheblichen Risiken für die Vertraulichkeit und Sicherheit der Daten verbunden sein kann.
Wie die Presse in den letzten Monaten ausführlich berichtet hat, betreiben ausländische Nachrichtendienste eine Reihe von Programmen (PRISM, Tempora), um Kommunikationsdienste weltweit abzuhören. Deutschland gehört zu den Ländern, in denen besonders intensiv Daten abgehört werden.

Forschungsdaten als Ziel von Wirtschaftsspionage
Begründet wurden die Abhöraktionen durch die Nachrichtendienste insbesondere mit der Notwendigkeit der Bekämpfung des internationalen Terrorismus. Dass aber auch wirtschaftliche Interessen mit den Spionageprogrammen verfolgt werden, ist nicht von der Hand zu weisen. Es muss davon ausgegangen werden, dass auch das Abschöpfen von Forschungsdaten und Forschungsergebnissen dazu zählt. Das ist insbesondere dann kritisch, wenn die Daten noch nicht publiziert worden sind oder durch Drittmittelforschung einer Geheimhaltung unterliegen.
Forschungs- und Wirtschaftsspionage sind kein neues Phänomen. Doch durch den rasanten Technologiewandel wird eine immer flächendeckendere Überwachung zu einem erheblichen Risiko für die Vertraulichkeit und Sicherheit Ihrer Forschungsdaten.

Daten werden insbesondere auf zwei Wegen gesammelt:

- Über Server der Dienste Google, Microsoft, Yahoo, Facebook, Skype, Apple, AOL und Paltalk. Ein Zugriff ist dabei auf E-Mails, Video- und VoIP-Chats, Fotos, und allgemein gespeicherte Daten möglich.
- Über ein direktes Mitschneiden des internationalen Datenverkehrs, unter anderem auf Glasfaserstrecken, über die auch ein Großteil des deutschen Datenverkehrs läuft.

Risiken bei der Nutzung von Kommunikationsdiensten

Grundsätzlich kann sämtlicher Datenverkehr, der unverschlüsselt über ein Netzwerk läuft, von Dritten mitgelesen werden. Daten, die ausschließlich über die internen IT-Systeme der Universität laufen, sind besser gegen ein Abhören durch Dritte geschützt. Dieser Schutz gilt beispielsweise für den Mailverkehr zwischen E-Mail-Adressen der Universität Bielefeld sowie Daten, die auf den zentralen Netzlaufwerken gespeichert werden. Sobald Anbieter außerhalb der Universität genutzt werden, muss davon ausgegangen werden, dass die Daten von unbefugten Dritten mitgelesen werden können. Von einer Vertraulichkeit der Daten kann nicht mehr ausgegangen werden. Dies trifft auch auf folgende Beispiele zu:

Beispiele für eine externe Verarbeitung von Forschungsdaten

- Eine externe Speichernutzung bei Diensten wie Skydrive, iCloud, Dropbox oder ähnlichen
- Eine Nutzung von externen Kommunikationsdiensten (Video- oder VoIP-Chat) zum wissenschaftlichen Austausch wie beispielsweise Skype oder FaceTime
- Eine (permanente) Weiterleitung von universitären E-Mails auf Adressen bei Fremdanbietern (zum Beispiel Gmail, Hotmail, iCloud, Yahoo)
- Die Nutzung von Online-Textverarbeitungen zur Erstellung und Bearbeitung von Forschungsdaten beispielsweise in Google Drive, Microsoft Office 365 oder Apple iCloud

Maßnahmen zur Erhöhung der Sicherheit von vertraulichen Forschungsdaten

- Für eine Verarbeitung von vertraulichen Forschungsdaten sind vorrangig die IT-Dienste der Universität Bielefeld zu nutzen. Vertraulich sind Forschungsdaten beispielsweise dann, wenn diese noch nicht publiziert worden sind, personenbezogene Daten enthalten oder einer vertraglichen Geheimhaltung unterliegen.
- Bei der Nutzung externer Dienste sind bevorzugt Anbieter aus dem deutschen Datenschutzraum auszuwählen. Die beispielhaft genannten Anbieter wie Skydrive, iCloud und Dropbox zählen nicht dazu.
- Vertrauliche Forschungsdaten sind **vor** einer Übertragung zu externen Anbietern zu verschlüsseln.

Software- und Anbieterempfehlungen zur Wahrung der Vertraulichkeit

Zur Verschlüsselung bieten sich je nach Anforderung unterschiedliche Lösungen an:

- Erstellung passwortgeschützter Zip-Dateien[1] beispielsweise mit 7-Zip oder Winzip
- Erstellung verschlüsselter Verzeichnisse, beispielsweise mit Truecrypt[2] oder Boxcryptor[3]
- Nutzung von externen Online-Speicher-Anbietern wie Teamdrive[4], welche die Daten vor einer Übertragung in die Cloud verschlüsseln und ein deutsches Datenschutzgütesigel tragen.
- Nutzung von Chat- und Videotelefonie-Software wie Jitsi oder Gajim[5], welche die Kommunikation anhand anerkannt sicherer Standards durchgängig verschlüsseln.

Weitergehende Anleitungen finden Sie unter den unten aufgeführten Links. Für technische Unterstützung wenden Sie sich bitte an den IT-Support Ihrer Fakultät oder Einrichtung.

Das Hochschulrechenzentrum der Universität Bielefeld beabsichtigt im kommenden Jahr, im Rahmen der Erweiterung von Speichersystemen, eine interne Online-Speicherlösung zur Kollaboration bereitzustellen.

Hinsichtlich der vorstehenden Ausführungen bitte ich um Kenntnisnahme, Beachtung und Bekanntgabe in Ihrem Bereich.

Gerhard Sagerer

Prof. Dr.-Ing. Gerhard Sagerer
Rektor der Universität Bielefeld

---

[1] http://www.zendas.de/technik/sicherheit/verschluesselung_fuer_jedermann/zipper.html
[2] Webseite: http://www.truecrypt.org; Anleitung: http://www.truecrypt.org/docs/tutorial
[3] Webseite: https://www.boxcryptor.com; Anleitung: https://www.boxcryptor.com/en/boxcryptor
[4] http://www.teamdrive.com/de und http://www.teamdrive.com/de/datenschutzguetesiegel.html
[5] http://www.jitsi.org/ oder http://www.gajim.org