Universität Bielefeld	IT-Sicherheitsrichtlinie zur Nutzung von Skype
Art: IT-Sicherheitsrichtlinie	Version: 1.0
Verfassende: Michael Sundermeyer	Freigabedatum: 21.06.2012
Zielgruppe: Mitarbeiterinnen und Mitarbeiter, IT-Personal	Letzte Änderung: 23.05.2012

1. Einleitung

Die Software „Skype“ kommt in vielen Bereichen zum Austausch von Informationen mittels Video-, Sprach-, Chat- und Datenübertragung zum Einsatz. Bei einer Nutzung von Skype bestehen Risiken für die Vertraulichkeit, Integrität und Verfügbarkeit der Daten. Aus diesem Grund wird eine dienstliche Nutzung von Skype nicht empfohlen. Sollte eine Nutzung aus zur Erledigung von Dienstaufgaben zwingend erforderlich sein, bildet diese Richtlinie einen verbindlichen Rahmen für die Beschäftigten und das IT-Personal der Universität Bielefeld. Basis für diese Richtlinie ist die aktuell gültige IT-Sicherheitsleitlinie der Universität Bielefeld.

2. Geltungsbereich

Diese Richtlinie ist allen Personen und Gruppen, die Skype administrieren und nutzen bekannt und gilt als verbindlicher Rahmen für die Nutzung und den Einsatz von Skype auf dienstlichen IT-Geräten der Universität Bielefeld.

3. Zuständigkeiten

Die IT- bzw. DV-Beauftragten der Fakultäten und Einrichtungen sind verantwortlich für die richtlinienkonforme Nutzung von Skype auf dienstlichen IT-Geräten der Universität Bielefeld. Für die Installation und Administration der Software ist die IT-Betreuung des jeweiligen Bereichs zuständig.

4. Regelungen

4.1 Allgemeines

- Die Nutzung von externen Kommunikationsdiensten ist auf dienstlichen IT-Geräten grundsätzlich nicht gestattet[1].
- Ausnahmen von dieser Regelung in Bezug auf die Nutzung von Skype sind möglich, sofern die Rahmenbedingungen dieser Richtlinie eingehalten werden. Dies ist durch technische bzw. organisatorische Maßnahmen sicher zu stellen, die in der Verantwortung des jeweiligen Bereichs liegen.
- Sofern eine Person ihren dienstlichen Rechner eigenständig mit Admin-Rechten verwaltet, trägt diese für die Konfiguration und Pflege der Software die Verantwortung.

4.2 Risiken

- Skype nutzt ein nicht veröffentlichtes, proprietäres Protokoll zur Verschlüsselung der Datenübertragung. Es ist unklar ob und wie widerstandsfähig dieses gegen Angriffe ist. Von einer Vertraulichkeit bei der Datenübertragung darf daher nicht ausgegangen werden. Für einen Austausch von vertraulichen dienstlichen Informationen ist Skype nicht geeignet.
- Skype kann Funktionen von Firewalls unterlaufen und somit Sicherheitsmaßnahmen im Netzwerk der Universität umgehen und außer Kraft setzen.

[1] Vergleiche „Regelungen zum IT-Basisschutz für IT-Anwenderinnen und Anwender“ vom 15.11.2011, Punkt M 20: Nutzung von externen Kommunikationsdiensten.

- Skype kann leistungsfähige Rechner mit einer schnellen Internetanbindung ohne Kenntnis der Inhaber als sogenannte „Supernode“ nutzen d.h. als Vermittlungsstation für andere Skype-Benutzer. Das öffnet den Rechner für fremden Datenverkehr und kann die Netzwerkressourcen und Rechnerleistung belasten.
- Die Funktionen von Skype können als Einfallstor für schädliche Software missbraucht werden. Ebenso kann Skype für Angriffe auf der sozialen Ebene (social engineering) missbraucht werden, indem Personen unter einer falschen Identität kontaktiert werden, um an vertrauliche Informationen zu gelangen Akzeptieren Sie einen Datenaustausch ausschließlich von und mit Personen, deren Identität ihnen zweifelsfrei bekannt ist.

4.3 Konfigurations- und Nutzungsvorgaben

- Der Rechner muss den Vorgaben der Regelungen zum IT-Basisschutz[2] genügen (insbesondere über einen aktuellen Software-Stand, aktuelle Antiviren-Software sowie eine aktivierte Firewall verfügen). Es ist sicher zu stellen, dass ausschließlich aktuelle Versionen von Skype zum Einsatz kommen. Sicherheitsrelevante Updates müssen umgehend installiert werden.
- Skype ist nur bei Bedarf zu starten, die Auto-Login Funktion der Software ist zu deaktivieren.
- Das Skype-Passwort darf nicht mit Passworten anderer Dienste der Universität Bielefeld identisch sein.
- Ein Austausch von vertraulichen dienstlichen Daten über die Datenübertragungsfunktion von Skype ist untersagt. Vertrauliche dienstliche Daten sind Informationen der Universität Bielefeld, die nicht für die Öffentlichkeit, sondern ausschließlich für einen internen und eingeschränkten Personenkreis bestimmt sind. Dazu zählen beispielsweise Daten mit Personenbezug (d.h. Daten die den Datenschutzgesetzen unterliegen), Finanzdaten oder auch Forschungsdaten, die nicht bzw. noch nicht publiziert worden sind.
- Die Supernode-Funktion von Skype ist zu deaktivieren.

Bei Fragen zu den Konfigurationsvorgaben wenden Sie sich bitte an die IT-Betreuung in Ihrem Bereich.

4.4 Ausschlusskriterien für den Einsatz von Skype

Um die Integrität, Vertraulichkeit und Verfügbarkeit von kritischen Rechnern und Daten gewährleisten zu können, ist der Einsatz von Skype unter folgenden Bedingungen untersagt:

- Rechner die technische Anlagen steuern.
- Rechner die Server-Funktionen erfüllen.
- Rechner die aus betrieblichen Gründen nicht den Anforderungen des IT-Basisschutzes genügen (fehlende Updates des Betriebssystems, keine Antivirus-Software, deaktivierte Firewall, schwache Passwörter etc.).
- Rechner die vertraulichen Daten wie beispielsweise personenbezogene Prüfungsdaten, Finanzdaten oder Forschungsergebnisse enthalten und damit einen hohen Schutzbedarf haben.

5. Umsetzung und Revision

Die Leitungen der Fakultäten und Einrichtungen tragen die Verantwortung für die Umsetzung dieser Richtlinie.

Der oder die IT-Sicherheitsbeauftragte trägt die Verantwortung für die Prüfung der Umsetzung dieser Richtlinie. Des Weiteren überprüft dieser die Richtlinie regelmäßig, jedoch mindestens einmal pro

[2] Vgl. Regelungen zum IT-Basisschutz für IT-Anwenderinnen und Anwender vom 15.11.2011: http://www.uni-bielefeld.de/it-sicherheit/Regelungen/Regelungen_IT-Basisschutz_Anwendende_2011-11-15.pdf

Jahr, auf Ihre Aktualität und Konformität mit den IT-Sicherheitsregelungen der Universität Bielefeld und überarbeitet diese gegebenenfalls.

6. Behandlung von Ausnahmen

Ausnahmen, die den Regelungen dieser Richtlinie widersprechen, sind mit dem oder der IT-Beauftragten des Bereichs abzustimmen und schriftlich an den oder die IT-Sicherheitsbeauftragte zu kommunizieren.