Deutsche Initiative für NetzwerkInformation e.V.

Video**K**onferenz**T**echnologien und ihre **A**nwendungs**S**zenarien
Arbeitsgruppe (AG) **VIKTAS**

– Warnung vor der Nutzung der Software Skype –

Die DINI AG VIKTAS rät aufgrund verschiedener Probleme von der Nutzung der Software Skype ab. Mit Ihrer Zustimmung zu den AGBs übertragen Sie als Nutzer der Firma Nutzungsrechte an Ihren Kommunikationsinhalten wie gesprochene Texte, Vortragsfolien, Bilder Videochat usw. Bedenken Sie dieses bitte, bevor Sie Skype installieren!

Softwarelösungen für Video- und Internettelefonie wie Skype, Google Hangout, Apples Facetime und weitere erfreuen sich großer Beliebtheit. Sie sind kostengünstige Lösungen, insbesondere wenn höhere Telefonkosten anfallen würden. Durch das Bild des Kommunikationspartners sind die Lösungen zusätzlich attraktiv. Diese Softwarelösungen sind firmenspezifisch. Daher sind Anrufe zu einem Partner, der eine andere Softwarelösung als Sie verwendet, meist nicht möglich.

Insbesondere Skype hat große Nutzerzahlen und verbreitet sich sehr leicht. Technische Raffinesse wird mit gekonntem Marketing verbunden. Der Einstieg ist leicht. Softwarelösungen dieser Art werden durch kommerzielle Firmen häufig sogar kostenfrei angeboten. Aber weder die Geschäftskonzepte der Firmen noch die Auswirkungen auf die Informations- und IT-Sicherheit sind offensichtlich.

Die Installation ist ein tiefer Eingriff in das Rechnersystem. Einmal installiert kann Skype Bandbreite, Netzwerkverbindungen und Rechenkapazität automatisch für unbekannte Dritte zur Verfügung stellen. Skype verfügt über eine Supernode-Funktionalität (eine Art Vermittlungszentrale), ein eigenes Skype-API und die Möglichkeit verschlüsselten Dateitransfers. Zwar lassen sich Funktionen deaktivieren, das erfordert jedoch Eingriffe in die Registry, was wenig nutzerfreundlich ist. Spätestens seit den Snowden-Veröffentlichungen mehren sich zudem Zweifel an der Wirksamkeit solcher Deaktivierungen.

Skype kann eine ganze Reihe verschiedener Wege im Netzwerk verwenden. Selbst etablierte Firewalls und auch andere technische Sicherungsmaßnahmen bieten noch immer keinen sicheren Schutz. IT-Security-Maßnahmen an Universitäten oder in Forschungsinstitutionen sind damit häufig wirkungslos.

Auf die **Installation** von Skype sollte daher **generell verzichtet** werden in Infrastrukturbereichen wie Rechenzentren, Gebäudemanagement/Leitwarte, Verwaltung und in anderen Bereichen, die schützenswerte Informationen wie Diplomarbeiten, Promotionsarbeiten, Patentanträge, Förderanträge oder Forschungsergebnisse vor der Veröffentlichung verarbeiten.

Auf Rechnern, die keine personenbezogenen Daten im Sinne des Datenschutzgesetzes oder andere schützenswerte Informationen verarbeiten und mit separaten Internetzugängen arbeiten, kann Skype toleriert werden.

In (separierten) Netzbereichen, die Internetzugänge für Studierende, Gäste oder Patienten bereitstellen, sollten jeweils Nutzen und Risiko gegeneinander abgewogen werden.

Rechenzentren, Helpdesks einer Universität oder Forschungsinstitutionen sollten mit ihren Ressourcen aufgrund dieser Problematik **keinen Support für Skype** leisten.

Im Deutschen Forschungsnetz sind als Alternative Webkonferenzen über die Server des DFN Vereins und die Nutzung von etablierten Videokonferenzräumen zu empfehlen.

AG VIKTAS des DINI e.V. Stand August 2015

Verfalls- bzw. Erneuerungsdatum dieses Textes: 31.07.2016

Dieser Text spricht vom populären „Consumer-Skype“, was zur Zeit noch streng zu trennen ist von „Skype for Business“ (dem Nachfolger von Microsoft Lync 2013) und kann, bei der zur Zeit raschen Entwicklung, nur eine Momentaufnahme technischer Bedenken sein.