



– Mögliche Risiken bei der Nutzung von 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 Video-chat usw. Bedenken Sie dieses bitte, bevor Sie Skype installieren!

Softwarelösungen für Video- und [Internettelefonie](#) wie Skype, Google Hangouts, Apples Facetime, WhatsApp-Videoanrufe und andere 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 mit einer Software zu einem Partner, der eine andere Software verwendet, meist nicht möglich.

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

Nicht zu verwechseln ist Skype (hier: „Skype for Consumer“) mit „Skype for Business“, welches den Nachfolger von Microsoft Lync 2013 darstellt und auf einem dedizierten Serversystem aufbaut. „Skype for Business“ kann in der Microsoft Cloud, auf eigenen Servern oder hybrid betrieben werden. Die grundsätzlichen Bedenken bzgl. der Informations- und IT-Sicherheit wie bei Skype bestehen nicht, allerdings muss bei Servern in der Microsoft Cloud an datenschutzrechtliche Aspekte gedacht werden. Falls eine Kopplung der eigenen „Skype for Business“-Infrastruktur mit der Microsoft Cloud vorgenommen wird (z.B. zur Anbindung an das Skype-Netzwerk), sind entsprechende Rufe zu Skype-Nutzern aber zumindest auf dem Weg von der Microsoft Cloud zu Skype und in der entgegengesetzten Richtung von den genannten Risiken betroffen.

„Skype for Web“ wird im Browser ausgeführt (als Plugin bzw. Nutzung von WebRTC) und wird daher nicht wie Skype als Anwendung auf dem Rechner installiert und läuft auch nicht die gesamte Zeit im Hintergrund mit. Eine Gastnutzung von „Skype for Web“ ohne vorherige Anmeldung ist möglich. Die Verbindung zur Microsoft Cloud ist aber technisch zur Herstellung der Rufe / Versendung des Chats etc. notwendig und so sind datenschutzrechtliche Aspekte zu beachten. Im Zweifelsfall ist es aus Gründen der Informations- und IT-Sicherheit aber besser Skype for Web anstatt von Skype zu nutzen.

Seit Windows 10 ist Skype generell vorinstalliert, aber auch die nachträgliche Installation bei älteren Systemen 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 zum verschlüsselten Dateitransfer. Zwar lassen sich Funktionen deaktivieren, dies 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 und Löcher in Firewalls öffnen. Selbst etablierte Firewalls und auch andere technische Sicherungsmaßnahmen bieten noch immer keinen sicheren Schutz. IT-Security-Maßnahmen an Universitäten oder Forschungsinstitutionen sind damit häufig wirkungslos.

Auf die **Installation** von Skype sollte daher **generell verzichtet** (im Notfall sogar deinstalliert) werden in Infrastrukturbereichen, wie Rechenzentren, dem Gebäudemanagement/Leitwarte, in der Verwaltung und in anderen Bereichen, wo schützenswerte Informationen, wie Diplomarbeiten, Promotionsarbeiten, Patentanträge, Förderanträge oder Forschungsergebnisse vor der Veröffentlichung verarbeitet werden.

Auf Rechnern, die keine personenbezogenen Daten im Sinn des Datenschutzgesetzes oder andere schützenswerte Informationen verarbeiten und mit separaten Internetzugängen arbeiten, kann Skype toleriert werden. In (separaten) Netzbereichen, die Internetzugänge für Studierende, Gäste oder Patienten bereitstellen, sollten Nutzen und Risiko jeweils gegeneinander abgewogen werden. Rechenzentren, Helpdesks einer Universität oder Forschungsinstitution sollten mit ihren Ressourcen **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.