Fraunhofer ESK

Einsatz von Skype im Unternehmen

Chancen, Risiken und Policy – Empfehlungen

Autor: Thomas Messerer
Weitere Autorin: Beate Eickhoff

Version: V 1.0

Datum: 28.11.2013

Inhalt

1 Einleitung

In den Unternehmen besteht weiterhin eine große Nachfrage zum Einsatz von Skype. Die vorhandene Studie (Version 2.0.1) zur Nutzung von Skype wurde unter Berücksichtigung der neuesten Skype-Version (6.3.0.107) überarbeitet. Es erfolgte eine Anpassung der gewonnenen Erkenntnisse und eine Überprüfung sowie ggf. eine entsprechende Aktualisierung der bisherigen Policy-Empfehlungen. Neben erweiterten Konfigurationshinweisen wurden die folgenden Aspekte bei der Überarbeitung berücksichtigt:

- Hinzugekommene Features
- Aktuelle Version der Endbenutzer-Lizenzvereinbarung
- Einstellmöglichkeiten bzgl. Supernodes
- Aktuelle Erkenntnisse zu Sicherheits- und Rechtsfragen

In Kap. 2 wird zunächst eine Zusammenfassung der Ergebnisse der Evaluation von Skype gegeben.
Die Kapitel 3 und 4 beschreiben anschließend die Funktionsweise von Skype und die für den Nutzer verfügbaren Leistungsmerkmale.
Welche Vorteile, aber auch Risiken, Skype aufweist wird in Kapitel 5 dargestellt.
Die Kapitel 6 und 7 gehen detailliert auf Sicherheits- und Rechtsfragen ein, bevor in Kapitel 8 eine auf den gewonnenen Erkenntnissen basierende Empfehlung für eine Skype-Policy mit entsprechenden Konfigurationshinweisen ausgesprochen wird.

2 Zusammenfassung

Der Internetdienst Skype steht in erster Linie für Telefonie über das Internet. Neben Telefonie ermöglicht er auch Telefon-Konferenzen mit bis zu 25 Personen, Desktop-Video-Telefonie (mit bis zu 10 Teilnehmer), Instant Messaging, Datei- und Bildschirmübertragung und gegen Entgelt auch Übergänge in klassische Telefonnetze. Skype-Clients sind für verschiedene Betriebssysteme auf Arbeitsplatzrechnern und auf mobilen Systemen (Notebook, Smartphone) verfügbar. Spezielle Skype-Telefone („RTX DUALphone 4088 und Grandstream GXV3140 IP Multimedia Phone“) sowie die Nutzung von Skype über Satellitentelefone und in TV-Geräten sind nicht Gegenstand dieses Papiers.

Skype basiert auf der Peer-to-Peer-Technologie (P2P). Der Vorteil von P2P-Systemen gegenüber traditionellen Client-Server-Netzwerken besteht in dem dynamisch erweiterbaren Netzwerk und der Dezentralisierung von Ressourcen, besserer Aufgabenverteilung und schlussendlich in Kosteneinsparung. Um Skype zu nutzen, muss man die kostenfreie Skype-Software laden und sich beim Skype-Server registrieren. Für die Nutzung des Dienstes werden Konfigurationsdaten, wie Zugangsdaten, Kontakt- und Präsenzinformationen gespeichert. Die Kommunikation erfolgt über ein Peer-to-Peer Netz. Dabei können Rechner von Skypenutzern unter bestimmten technischen Voraussetzungen zum Verteilen der Konfigurationsdaten und zum Verbindungsaufbau (Supernodes) sowie als Zwischenstationen der Übertragung (Relay) genutzt werden.

Seit der Version 3.0 ermöglicht Skype vermehrt Funktionen, die für einen Einsatz in Unternehmen relevant sind. Aufgrund von geäußerten Sicherheitsbedenken der Firmen wurden zusätzliche Konfigurationsmöglichkeiten durch den Hersteller geschaffen. Dazu gehören u.a. die Bereitstellung eines Windows Installer Pakets, die Möglichkeiten zur Konfiguration von Skype über Windows Registry Keys, sowie ein kostenloses Control Panel für Unternehmen zur Verwaltung von Skype-Guthaben und Zuweisung von SkypeIn-Nummern. Außerdem wurde ein Leitfaden für Netzwerkadministratoren veröffentlicht[1].

Schon aufgrund der nicht vorhandenen Notruffunktion, nicht garantierbarer Verfügbarkeit, und netzabhängigen Qualitätseinbußen ist Skype kein Ersatz für die klassische Telefonie im Unternehmen. Einige Merkmale, wie verschlüsselte Video- und Telefonkommunikation, ad-hoc Konferenzen und Präsenzinformationen sind jedoch auch in der Geschäftswet – beispielsweise für kollaborative Projektarbeit mit externen Partnern – interessant und werden bereits genutzt. Vorteile von Skype gegenüber SIP und herkömmlicher Telefonie liegen in den genannten Merkmalen sowie der einfachen Installation und Nutzung über verschiedene Systemplattformen hinweg.

Ein Kritikpunkt ist, dass die von Skype eingesetzten Protokolle nicht offen gelegt sind und dass der Code der Software keiner Überprüfung zugänglich ist, so dass Sicherheitskonzepte und deren Implementierung nicht überprüfbar sind. Über Skype könnten Firmendaten nach außen geschleust werden, ohne dass auch nur die Chance einer Kontrolle bestünde.

Die ist insbesondere durch die aktuell in den Medien veröffentlichen Fakten zu Abhörmöglichkeiten durch die NSA und andere Sicherheitsbehörden sehr in der Diskussion.

[1] Downlod der jeweils aktuellsten Version über http://download.skype.com/share/business/guides/skype-it-administrators-guide.pdf,

Die Tunnelung der Firewall macht die IT-Infrastruktur verwundbarer.

Die Kritik an Skype ist berechtigt, die Risiken sind aber abzuwägen. Im Vergleich zu den Risiken weitgehend ungeschützter herkömmlicher Telefonie ist auch eine nicht überprüfbare Verschlüsselung vorteilhaft, da diese gegen Abhören schützt und so die Vertraulichkeit der Kommunikation erhöht. Letztendlich müssen die in der offenen Kommunikation zunehmenden Risiken durch Wachsamkeit und durch verstärkte Sicherheitsanstrengungen auf den Endgeräten angegangen werden.

Im Ergebnis eines Diskussionsprozesses wird deshalb die in Kap. 8 beschriebene Policy vorgeschlagen.

3 Was ist Skype?

Das Client-Programm von Skype vereint mehrere Kommunikationsfunktionen und ist weit verbreitet. Eine funktionierende Internet-Verbindung vorausgesetzt, lässt es sich durch den Benutzer einfach herunterladen, installieren und auf vielfältigen Plattformen nutzen. Im Hintergrund steht ein nicht transparenter, proprietärer Internet-Service. Skype hat sich – wie viele Internet-Services – über die privaten Anwender verbreitet und hat dort in erster Linie seinen Fokus Durch „Skype Connect" und „Skype Manager" wird aber auch die Verbreitung von Skype im Enterprise Umfeld vom Anbieter gefördert. Für die Beliebtheit von Skype sprechen die Nutzungszahlen. Die Skype-Gemeinde zählt inzwischen über 650 Mio. User, wovon im Durchschnitt ständig ca. 55 Mio. online sind.

Die ursprüngliche Firma Skype Inc. wurde 2005 von eBay Inc. gekauft. Anfang 2009 wurden Lizenzstreitigkeiten zwischen eBay und Joltid Limited, der Firma mit den Rechten an zentralen Skype-Technologien, bekannt. Im September 2009 veräußerte eBay 65% von Skype an eine Gruppe von Venture-Capital- und Private-Equity-Unternehmen. Anschließend wurde auch der Rechtsstreit über potentielle Lizenzverletzungen beigelegt. 2011 hat Microsoft für 8,5 Milliarden US-Dollar den Dienst übernommen. Skype ist somit eine 100- prozentige Tochtergesellschaft von Microsoft.

Hauptfokus des Dienstes ist die einfache Sprach- und Video-Telefonie über das Internet mit relativ neuen Zusatzfunktionen. Zum Installieren des Skype-Anwendungsprogramms braucht es keine Administrationsrechte, das Skype-Programm setzt vollständig auf die Funktionen der bestehenden Arbeitsumgebung (u.a. Mikrofon, Lautsprecher, Kamera) des Users auf. Der Benutzer kann völlig autonom, unabhängig von der IT-Administration die Entscheidung über die Nutzung oder Nichtnutzung von Skype treffen. Nach erfolgreichem Abschluss der Installation entstehen außer den Internet-Nutzungskosten im Standardfall keine weiteren Kosten. Skype bietet seinen Nutzern folgende kostenfreie Kommunikationsdienste:

- Sprachtelefonie
- Videotelefonie
- Sprachkonferenzen mit bis zu 25 Personen
- Videokonferenzen mit bis zu 10 Personen
- Instant Messaging inkl. Konferenzen
- Austausch von Dateien
- Bildschirmfreigabe

Als anwählbare Kommunikationsadressen dienen Skype-Benutzernamen, die der registrierte Benutzer frei wählen kann. Für die Verwaltung von Kontakten und zur Steuerung der Kommunikation bietet Skype ferner folgende Merkmale:

- Anzeige differenzierter Präsenzinformation: Wer möchte kann seinen Status für andere Nutzer als erreichbar oder abwesend kennzeichnen. Es gibt sieben verschiedene Statusoptionen. Unerwünschte Benutzer können blockiert werden.

- Anzeige von Outlook-Kontakten mit integrierten Kommunikationsfunktionen: Persönliche Kontakte aus Outlook können einfach ein- und ausgeblendet werden, entsprechende Adressdaten sind dann direkt über Skype bzw. über SkypeOut (s.u.) anwählbar.
- Direkte Annahme: Nachrichten, aber auch Sprach- und Videoverbindungen können automatisch angenommen werden, ohne dass es dafür einer Interaktion bedarf.
- Kommunikation mit Gruppen: Für Konferenzen können Gruppen mit den betreffenden Kontakten in der eigenen Kontaktliste angelegt werden. Dadurch wird bei wiederkehrenden Konferenzen eine schnelle Initiierung möglich.

Neben den kostenfreien Funktionen gibt es kostenpflichtige Premium-Services, für die ein Benutzer ein eigenes Konto mit entsprechendem sog. Skype-Guthaben einrichten muss. Dies sind:

- SkypeOut: Ermöglicht kostenpflichtige Anrufe zu Festnetz- und Mobilanschlüssen.
- Skype-Nummer: Über eine gesondert vergebene eigene und lokale Nummer („Online-Nummer“) kann ein Teilnehmer von jedem beliebigen Festnetz- und Mobilfunkanschluss aus angerufen werden.
- Skype Voicemail: Beantwortet Anrufe wenn man nicht erreichbar ist, die gespeicherten Nachrichten können von überall aus abgerufen werden. Außerdem ist das Versenden von Sprachnachrichten möglich.
- Skype SMS: Ermöglicht das Senden von SMS-Nachrichten an SMS-fähige Endgeräte.
- Skype WiFi: Weltweiter WLAN-Hotspot-Zugangsservice der bspw. an Flughäfen und in Hotels genutzt werden kann. Der Skype-Client erkennt, ob verbundene Hotspots die Abrechnung über Skype-Guthaben erlauben. Falls dem so ist, erfolgt eine minutengenaue Abrechnung.

Speziell für den Einsatz in Unternehmen wurden die beiden folgenden Komponenten entwickelt:

- Skype Manager: Webbasiertes Tool, das die zentrale Verwaltung von Skype-Guthaben und Online-Nummern für verschiedene Benutzer ermöglicht.
- Skype Connect: Möglichkeit zur Integration von Skype-Funktionen mit bestehenden TK-Anlagen (nur bestimmte Hersteller werden unterstützt). Es können bspw. Click-to-Call Applikationen oder Zuweisungen von Online-Nummern und internen Nebenstellen realisiert werden. Kunden oder Partner können dann über Schaltflächen auf der unternehmseigenen Webseite oder in E-Mails kostenlose Skype-Anrufe initiieren, die direkt an bestimmte Mitarbeiter geleitet werden. Des Weiteren können Skype-Telefonate über bestehende Tischtelefone geführt werden, um bspw. bei Auslandsgesprächen von günstigen Skype-Out Konditionen zu profitieren oder um reisende Projektpartner auch unterwegs anzurufen.

4 Wie funktioniert Skype?

4.1 Client-zu-Client-Kommunikation

Die meisten Kommunikationsservices in Firmennetzen beruhen heute auf dem Client-Server-Modell: Ein Client ruft über definierte Schnittstellen definierte Services ab. Dieses Modell hat sich in der IT-Welt Ende der 80-er/Anfang der 90-er Jahre durchgesetzt.

Mit dem PC als dem Repräsentanten des Users (und inzwischen verschiedene Mobile Devices als weiteren Repräsentanten) entstand insbesondere durch das Zusammenwachsen der Telefonie- mit der Datenwelt immer mehr der Wunsch nach einer direkten Kommunikation zwischen den Partnern ohne eine zwischengeschaltete zentrale Instanz. Die konzeptionelle Antwort wird unter dem Begriff „Peer-to-Peer-Netze" (P2P) zusammengefasst. Da der Desktop bzw. der genutzte Client die konkrete Benutzerumgebung – die Repräsentanz – des eigentlichen Nutzers ist, lässt sich der Kern dieser Entwicklung besser mit dem Begriff Client-zu-Client-Kommunikation charakterisieren.

Typische Merkmale solcher Client-zu-Client-Kommunikationslösungen sind, dass sie die bekannten Firewall-Techniken zur Analyse von Datenströmen kennen und bewusst nutzen, die Ressourcen der konkreten Arbeitsumgebung des Users selbständig analysieren und daraus ableiten, wie die zur Kommunikation nach außen frei geschalteten Ports (dynamisch) genutzt werden können (Firewalls tunneln). Die Kontrollmöglichkeiten für einen Dritten sind dadurch dramatisch eingeschränkt.

Die Vorteile der P2P-Netze liegen in ihrer dezentralen Infrastruktur. Diese Netzwerke können beliebig erweitert werden ohne dass die Performance leidet bzw. eine zentrale Infrastruktur bereitgestellt werden muss. Es werden die Ressourcen aller Anwender zur Bearbeitung der Aufgaben herangezogen. Um jedoch die für die Echtzeitkommunikation notwendige Qualität zu erreichen, mussten die ursprünglichen P2P-Netzwerke angepasst werden. Skype baut daher auf eine P2P-Technologie der dritten Generation („3G P2P"), den so genannten Global Index (GI). Die GI-Technologie besteht aus einem mehrschichtigen Netzwerk, in dem sog. „Superknoten" so miteinander kommunizieren, dass jeder Knoten im Netzwerk mit minimaler Latenzzeit weiß, welche Benutzer und Ressourcen verfügbar sind.

4.2 Funktionsweise des Skype-Netzes

Skype ist zwar im Prinzip ein Peer-to-Peer-Netz, allerdings sind im Netz auch so genannte Supernodes vorhanden, über die zwei Benutzer miteinander Kontakt aufnehmen können. Während im Jahr 2004 über Analysen die Struktur des damaligen Skype-Netzes erfasst wurde, gibt es keine Informationen zur aktuellen Struktur. Der Grund dafür ist, dass Microsoft nach dem Kauf von Skype dessen Architektur geändert hat. Laut Microsoft wurden die Änderungen an der Netzarchitektur durchgeführt, um die „user expierence" zu verbessern, allerdings gibt es auch andere Informationen dazu. (siehe Kapitel 6.2)

5 Vor- und Nachteile von Skype

Die Features und Funktionsweise von Skype bieten seinen Nutzern gegenüber herkömmlichen Kommunikationsservices (ISDN-Telefonie, VoIP mit SIP, Instant Messager) zahlreiche Vorteile, weisen aber auch Nachteile und Risiken auf.

5.1 Vorteile

- Kostenfreie Nutzung: Skype ist ein kostenloses Programm. Die Kommunikation zwischen Skypenutzern ist – anders als die herkömmliche Telefonie – kostenlos und verursacht allenfalls Internet-Nutzungskosten beim Internet-Provider. Die durch den Dienst beanspruchte Bandbreite ist trotz guter Sprachqualität relativ gering.
- Plattformunabhängigkeit: Skype funktioniert auf den meisten Betriebssystem-Plattformen: Windows, Mac OS X und Linux. Auch für mobile Geräte existieren Applikationen. Diese sind jedoch teilweise funktional eingeschränkt. Zum einen, weil viele Mobilfunkprovider keine VoIP-Gespräche über ihre Netze zulassen, zum anderen weil die Skype Software nicht auf allen Endgeräten parallel mit anderen Programmen laufen kann (so ist etwa auf dem iPhone erst ab Iphone 3GS Multitasking möglich).
- Problemlose Installation ohne Admin-Rechte: Das Programm kann leicht heruntergeladen und problemlos installiert werden. Die Installation funktioniert – anders als bei vielen anderen derartigen Tools – auch ohne Administrationsrechte.
- Einfache Bedienung: Die Oberfläche ist einfach und intuitiv bedienbar. Es gibt benutzerfreundliche Hilfen zur Konfiguration von Headset und Kamera.
- Integration vielfältiger Kommunikationsservices: Skype ist eine Anwendung für Telefonie, Videotelefonie, Chat, Dateitransfer, Telefonkonferenzen (bis zu 25 Teilnehmer), Videokonferenzen (bis zu 10 Teilnehmer), Kontaktverwaltung und Screen Sharing. Alle Dienste können direkt vom Rechner am Arbeitsplatz genutzt werden.
- Der verwendete Codec bietet selbst bei sehr geringer verfügbarer Bandbreite eine bessere Sprachqualität als vergleichbare VoIP-Programme.
- Erreichbarkeitssteuerung und Anwesenheitsinformationen (Presence). Die Freigabe und die Anzeige der Presence-Information kann der Nutzer steuern, der Benutzer hat Zugriff auf die Presence-Information seiner Kontakte. Die Buddy-List ist eine individuell zu definierende Sicht auf die Kommunikationsfavoriten.
- Problemlose Funktion auch hinter Netzwerk-Firewalls: Die Applikation kennt die Firewall-Techniken zur Kontrolle von Datenströmen, analysiert die konkrete Benutzerumgebung und konfiguriert sich automatisch so, dass sie z.B. trotz Firewall- und NAT-Techniken funktioniert. Eine Ausnahme bilden lokale, persönliche Firewalls, die auf dem Computer eines Mitarbeiters installiert werden und Applikationen den generellen Zugriff auf Ressourcen wie bspw. die Internetverbindung verbieten. Eine solche Lösung könnte zwar die Skype-Nutzung verhindern, ist aber im Unternehmenseinsatz aufgrund des hohen Administrationsaufwands nicht praktikabel.

- Möglichkeit anonymer und pseudonymer Kommunikation: Um sich bei Skype zu registrieren, muss zwar unter anderem eine E-Mail-Adresse angegeben werden. Die Richtigkeit der Daten wird jedoch nicht überprüft. Bei der Registrierung für den Skype-Dienst kann man selbst entscheiden, wie viele Informationen man über sich selbst bekannt geben will. Im Minimum wird nur der frei wählbare "Nickname" nach außen sichtbar. Diese Anonymität des Gesprächspartners kann allerdings auch als Nachteil gewertet werden.
- Verschlüsselung: Die Kommunikation zwischen den Teilnehmern ist verschlüsselt.

5.2 Nachteile

Den genannten Vorteilen stehen aber auch Nachteile gegenüber:

- Fehlende Standardisierung, fehlende Interoperabilität: Die verwendeten Protokolle sind proprietär (z.B. nicht SIP-konform). Es gibt (noch) keine Standardisierung, vor allem noch keine Interoperabilität zu ähnlichen Ansätzen, wie z.B. anderen Instant-Messenger-Lösungen. Die Kommunikation bleibt – die kostenpflichtige Verwendung der Gateways für die Telefonie ausgenommen – auf Skype-Nutzer untereinander und Skype-Programme beschränkt.
- Das Skype-System ist eine geschlossene Gemeinschaft, Schnittstellen bspw. zu Verzeichnisdiensten sind nicht vorgesehen. Dadurch müssen Skype-Nutzer Kontakte manuell verwalten und können nicht auf die Einträge im Unternehmensadressbuch zurückgreifen.
- Die Leistungsmerkmale von Skype für die Telefonie reichen nicht an die von Telefonanlagen heran. Merkmale wie Chef-Sekretärfunktion, Heranholen von Gesprächen, Notrufe mit automatischem Verbindungsaufbau etc. gibt es nicht.
- Die Sprachqualität reicht nicht an die klassische ISDN-Telefonie heran.
- Bereitstellung der eigenen Ressourcen für die Skype-Community, d.h. der verwendete PC kann als Supernode oder Relay arbeiten, wobei ein nicht unerheblicher Datenverkehr über den PC laufen kann. Dies ist so auch in der Lizenzvereinbarung geregelt. In manchen Fällen können Rechner nicht zu Supernodes werden: Computer, die sich in einem Netzwerk hinter einem NAT-Gerät, einer restriktiven Firewall, oder einem http- oder SOCKS5-Proxy befinden, werden nicht zu Supernodes. Außerdem kann diese Eigenschaft explizit ausgeschlossen werden (siehe Kapitel 8).
  Zwar gibt es Meldungen, dass Client-PCs nicht mehr als Supernode genutzt werden, sondern dass Skype eigene Server dafür in der Architektur eingerichtet hat[2], dennoch sollte die Nutzung des eigenen PCs als Supernode in jedem Fall ausgeschlossen werden.
- Eingeschränkter Support: Bei Problemen mit der Software ist eine Kontaktaufnahme mit dem Hersteller nur per E-Mail möglich, telefonische Anfragen zur Problemlösung können nicht gestellt werden. Auch dieser Punkt spricht für eine nur ergänzende Verwendung von Skype in Kombination mit dedizierten Telefoniesystemen.

[2] http://winfuture.de/news,69474.html

- Die Parallel-Nutzung von mehreren Skype-Clients kann auch negative Auswirkungen haben, bspw. wenn unbefugte Nutzer, die Zugang zu Account-Daten bekommen, eine Chatsitzung mitlesen können.
- Es ist keine vollständige Kontrolle bzw. Blockade der Skype-Nutzung möglich. Bisherige Ansätze[3] zur Erkennung von Skype im Netzwerk sind aufgrund der dynamischen Routenwahl des Skype-Traffics oft nur begrenzt einsetzbar:
    - Erkennung und Blockierung der spezifischen UDP-Kommunikation beim Aufbau der verschlüsselten Verbindung, Skype ist jedoch nicht auf UDP angewiesen. (Biondi & Desclaux, 2006)
    - Bei aufgebauter TCP-Verbindung können die ersten zwei Pakete entschlüsselt und erkannt werden. (Desclaux, 2005)
- Die unklare Situation der Datensicherheit: Es gibt aktuell etliche Meldungen über Abhörmöglichkeiten bei Skype in Zusammenarbeit mit Sicherheitsbehörden (Siehe Kapitel 6.2)

[3] Eine Übersicht zu bisherigen Versuchen existiert unter: http://www1.cs.columbia.edu/~salman/skype

6 Sicherheitsaspekte

Ein Großteil der Kritik an Skype betrifft Sicherheitsaspekte. Leider gibt es von Herstellerseite nur wenig offizielle Informationen zur System- und Protokollspezifikation. Aufgrund der proprietären Kommunikation und Infrastruktur sind eigene Analysen nur sehr begrenzt durchführbar. Seriöse Aussagen sind demzufolge schwer möglich. Auch die große VoIP-Studie des BSI (BSI, 2005) geht nicht auf Skype ein, und es gibt auch aktuell vom BSI keine Aussagen. Andererseits bietet ein proprietärer Ansatz weniger Angriffsfläche für gezielte Angriffe von Hackern, da Schwachstellen weitaus schwerer zu entdecken sind. Besonders wenn Code und Protokolle verschlüsselt werden. Die bisherigen Diskussionen um Skype sowie eigene Überlegungen ergeben folgendes Bild:

6.1 Unklare Sicherheit (fehlende Offenlegung der Infrastruktur und Protokolle)

Die Kommunikationsinfrastruktur ist nicht offen gelegt. Ihre Funktionsweise im Front- als auch im Backendbereich ist nicht transparent.insbesondere nach den Änderungen, die Microsoft nach dem Kauf von Skype an der Netzarchitektur durchgeführt hat. Man ist auf Herstelleraussagen, Black-Box-Tests und Spekulationen angewiesen. Die Sicherheit der Protokolle, der Skype-Infrastruktur und des Skype-Clients kann deshalb nicht zuverlässig bewertet werden. Schwachstellen im Systemkonzept und der Implementierung von Sicherheitsfeatures sind nicht auszuschließen. Dies könnte Angreifern beispielsweise ermöglichen, die Kommunikation trotz der angegebenen Verwendung sicherer RSA- und AES-Verschlüsselungsalgorithmen abzuhören oder über einen unsicheren Update-Mechanismus Trojaner zu installieren.

Hinter der fehlenden Offenlegung der Protokolle können ökonomische Interessen vermutet werden, um einen Nachbau der Software und damit alternative Angebote zu verhindern. Dass der Skype-Hersteller Sicherheitsschwachstellen oder Falltüren absichtlich eingebaut hat, ist nicht anzunehmen.
Es ist aber davon auszugehen, dass Skype Strafverfolgungsbehörden und Geheimdiensten, etwa im Zuge der Terrorismusbekämpfung, Nutzerdaten bereitstellen kann und eine Möglichkeit eröffnet, die Verschlüsselung in solchen Fällen auszuhebeln oder in Rechner überwachter Skype-Nutzer einzudringen[4]. Dazu steht im „Skype Privacy Statement“: „Except as provided below, Skype shall not sell, rent, trade or otherwise transfer any Personal and/or Traffic Data or Communications Content to any third party without Your explicit permission, unless it is obliged to do so under applicable laws or by order of the competent authorities.“

Dass Geheimdienste abgehörte Nachrichten auch für Wirtschaftsspionage nutzen, wird immer wieder vermutet und auch vom Bundesamt für Verfassungsschutz bestätigt

Insofern ist im Zusammenhang mit den unter 6.2 aufgelisteten Punkten bei der geschäftlichen Nutzung von Skype durchaus ein Sicherheitsrisiko zu identifizieren.

[4] Hinweise dazu sind hier zu finden: http://cryptome.org/isp-spy/skype-spy.pdf

6.2 Überwachung des Nutzers und der Kommunikation

Durch Manipulation der Software, Sicherheitslücken oder Passwortdiebstahl kann die Kommunikation überwacht, Daten von der Festplatte des Nutzers oder aus dem lokalen Netz abgefragt, Rechnermikrophon und Kamera eingeschaltet und Räume belauscht werden. Gezielte Softwaremanipulationen mit den genannten Auswirkungen sind jedoch sehr unwahrscheinlich, schon weil sich der Code der Analyse entzieht, um gezielt einzugreifen. Vorstellbar ist aber, dass sowohl für polizeiliche / geheimdienstliche Überwachungsmaßnahmen als auch für Zwecke der Wirtschaftsspionage die notwendigen Daten bereitgestellt werden können.

Microsoft hat Änderungen in der Skype-Architektur vorgenommen. [5]

Demnach haben die Supernodes jetzt auch die Fähigkeit, nicht nur Signalisierungsdaten, sondern auch Sprachdaten zu routen, um es für die Überwachungsbehörden einfacher zu machen, die Gespräche zu monitoren. Die Meldung dazu wurde von Microsoft per DMCA (Digital Millennium Copyright Act) allerdings wieder aus dem Netz genommen.

Das US-Patent 20110153809 „Legal Interception" [6] deutet darauf hin, dass damit auch das Abhören von Skype ermöglicht werden soll.

Laut der Webseite [7] wurde der Verbindungsaufbau dahingehend geändert, dass in einem bestimmten Modus die Schlüsselaushandlung nicht mehr beim Nutzer, sondern bei Skype/Microsoft erfolgt. Mit diesen Schlüsseln kann dann die abgehörte Kommunikation der Nutzer entschlüsselt werden.

Skype liest offensichtlich alle Chat-Nachrichten mit, da im Mai 2013 entdeckt wurde, dass https-Links die in Chat-Nachrichten versandt wurden, anschließend von Skype/Microsoft aufgerufen wurden. In der Meldung von Heise [8] ist dieses Verhalten dokumentiert und näher erläutert; inzwischen wurde das Aufrufen der Links jedoch abgestellt.

Laut einem Bericht der „New York Times" arbeitet Skype bereit seit 2008 mit US-Geheimdienst-Behörden zusammen. [9] Das „Project Chess" wurde damals eingerichtet, um die Erkundung von Skype-Kommunikation für Strafverfolgungs- und Sicherheitsbehörden besser verfügbar zu machen, so die „New York Times".

Nach anderen Meldungen findet eine Zusammenarbeit im Rahmen des PRISM-Projekts seit 6.2.2001 statt.[10]

Nach neuesten Meldungen kann PRISM Skype-Anwender offenbar auch in Echtzeit überwachen:[11]

---

[5] (http://www.extremetech.com/computing/132935-microsoft-tweaking-skype-to-facilitate-wiretapping),

[6] http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&f=G&l=50&d=PG01&p=1&S1=20110153809&OS=20110153809&RS=20110153809

[7] http://rt.com/news/skype-wiretapping-intelligence-agencies-237/

[8] http://www.heise.de/security/meldung/Vorsicht-beim-Skypen-Microsoft-liest-mit-1857620.html

[9] http://www.nytimes.com/2013/06/20/technology/silicon-valley-and-spy-agency-bound-by-strengthening-web.html?_r=0

[10] http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data?guni=Network%20front:network-front%20main-2%20Special%20trail:Network%20front%20-%20special%20trail:Position1

Die NSA soll schon lange in Software von Microsoft „Hintertüren“ eingebaut haben, um Überwachungsmöglichkeiten zu haben und nach neuesten Meldungen auch Möglichkeiten geschaffen haben, um dem Geheimdienst etwa die Umgehung der eigenen Verschlüsselung für Chats oder für Emails zu ermöglichen. [12]

6.3 Fehlende Authentizität

Identitätsangaben bei der Registrierung werden nicht geprüft, die anzugebende E-Mail-Adresse muss nicht zwingend vorhanden sein. Wer sich hinter einem Benutzernamen verbirgt und ob veröffentlichte Kontaktangaben stimmen, kann nicht zweifelsfrei überprüft werden. Ein Angreifer, der das Passwort erfährt, kann unter falscher Identität kommunizieren.

Aufklärung über die Risiken – etwa in einer Belehrung – ist eine ausreichende Maßnahme.

6.4 Verschlüsselung

Bei Skype wird die komplette Kommunikation verschlüsselt. Das gilt sogar für Gespräche in das herkömmliche Telefonnetz zwischen Nutzer und Telefongateway. Ist das Gespräch in das Telefonnetz durchgeleitet worden, entfällt die Verschlüsselung, da das normale Telefon technisch nicht in der Lage ist, eine Entschlüsselung vorzunehmen. Die Verschlüsselung ist notwendig, da Skype die Peer-to-Peer-Technologie nutzt und Kommunikationsdaten auch über andere (Desktop-)Rechner laufen. Allerdings vertraut Skype jedem Computer, der Skype verwendet bzw. Skype-konform agiert, das schließt Supernodes und Relays mit ein. So könnte es sein, dass auf diese Weise unberechtigte Dritte Zugang zu Informationen erlangen könnten.

Skype verwendet für die Verschlüsselung der Daten AES (Advanced Encryption Standard; "Rijndael") mit 256-Bit-Schlüssel. Die symmetrischen AES-Keys werden mit RSA-Keys (1536 bis 2048 Bit) ausgehandelt. Die Details dagegen sind nicht offiziell bekannt.

Es besteht die Möglichkeit mit intelligenten Spoofingattacken, Man-in-the-Middle-Angriffe gegen die Verschlüsselung zu fahren, d.h. Daten umzuleiten und unbemerkt von den Gesprächspartnern umzuverschlüsseln.

Die verschlüsselte Kommunikation ist ein Alleinstellungsmerkmal von Skype. Im Vergleich dazu wird bei der gängigen VoIP-Telefonie per default nicht verschlüsselt. Eine nicht 100% sichere Verschlüsselung ist jedoch besser als keine.

6.5 Kanal zum Schmuggeln vertraulicher Unternehmensdaten

Weil die Unternehmensfirewall getunnelt und der Informationsfluss verschlüsselt wird, kann Skype verwendet werden, um unbemerkt Daten aus dem Unternehmen zu schleusen. Aktivierte

[11] http://www.heise.de/newsticker/meldung/Bericht-PRISM-ueberwacht-in-Echtzeit-1908878.html
http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

[12] http://www.heise.de/tp/artikel/39/39499/1.html

Trojaner könnten z.B. große Datenmengen verschlüsselt nach außen versenden. Schließlich kommen auch bösartige Mitarbeiter in Betracht. In all diesen Fällen gibt es keine Möglichkeit, den Datenstrom an einer Firewall oder Proxy bei Verdacht zu kontrollieren. Von Kritikern wird Skype deshalb als „perfektes Werkzeug zum anonymen Schmuggeln von Daten" und die „perfekte Backdoor" bezeichnet.

Für bösartige Mitarbeiter gibt es neben Skype viele Kanäle, Daten unbemerkt und unkontrollierbar aus dem Unternehmen nach außen zu schmuggeln, etwa verschlüsselte E-Mails oder USB-Sticks. Skype wegen dieser Möglichkeit zu unterbinden erscheint wenig zweckmäßig. Vielmehr ist der Zugriff auf vertrauenswürdige Daten unternehmensintern zu schützen und auf inhaltlich berechtigte Personen einzugrenzen. In Bereichen, in denen besondere Maßnahmen ergriffen werden müssen, um den versehentlichen oder missbräuchlichen Datentransport nach außen zu verhindern, ist Skype zu verbieten. Es sind dann aber auch andere Maßnahmen – etwa die Sperrung von USB-Ports und Laufwerken, das Verbot der Mailverschlüsselung etc. – zu ergreifen.

6.6 Datenschutz

Skype schützt die Privatsphäre. Durch Einstellungen im Skype-Client können die Kommunikationspartner eingeschränkt werden. Es besteht auch die Möglichkeit, bestimmte Benutzer zu blockieren. Diese Möglichkeiten bestehen bei der herkömmlichen Telefonie nicht.

Skype speichert für eigene Zwecke u. a. folgende Informationen (aus „Skype Privacy Statement"):

- Register Information
- User Profile
- Personal Data of friends
- Passive Information
- E-Mail adresses
- Subscriber Information (u.a. Bankdaten zum Abrechnen der kostenpflichtigen Dienste)
- Traffic Data

Profile, Verbindungs- und Erreichbarkeitsdaten werden zwischen den Supernodes ausgetauscht, um eine ortsunabhängige Nutzung von Skype zu gewährleisten.

Die Bereitstellung der Präsenzinformationen kann vom Nutzer gesteuert werden. Allerdings ist damit eine Überwachung beispielsweise der Anwesenheit am Arbeitsplatz durch autorisierte Kontakte möglich. Der Umgang mit Präsenzinformationen ist kein Skype-spezifisches Problem und sollte zukünftig generell geregelt werden.

6.7 Belastung des Netzes

Vor den Änderungen der Netzarchitektur durch Microsoft konnte jeder Rechner mit öffentlich zugänglicher IP-Adresse und installiertem Skype-Client zum Supernode oder Relay werden. Hieraus konnten sich unerwünschte Belastungen und Überlastungen bis hin zu Problemen bei der Internetanbindung ergeben.

Inwieweit es trotz der Änderungen zu Überlastproblemen auf Rechnern oder im Netz kommen kann, ist nicht bekannt.

Belastungsprobleme muss man beobachten, bisher wurdenl keine problematischen Auswirkungen bekannt, was wiederum nicht heißt, dass keine entstanden sind..

6.8 Gefährdung der Netze über die Endgeräte

Nach der Anmeldung besteht durch die Firewall eine Verbindung zum Skype-Netz. Angreifer könnten versuchen, durch die Firewall hindurch DOS-Attacken direkt gegen den Host zu führen oder in den Host einzudringen, indem sie Fehler der Skypesoftware nutzen (etwa Buffer overflow Attacken). Es ist denkbar, dass Angreifer die Skypeinfrastruktur nutzen, um Viren oder Trojaner zu verbreiten.

Fehler in der Skypesoftware, die es ermöglichen Code auf dem Zielrechner auszuführen, hat es schon gegeben. Diese wurden jedoch schnell behoben. Das Risiko ist größer als bei herkömmlichen Internetanwendungen, bei denen die Endsysteme nicht direkt erreichbar sind. Gänzlich einzigartig sind sie jedoch nicht. Verschlüsselte infizierte Mail erreicht ebenfalls die Endsysteme, hier hilft auch kein Mailgateway. Man muss strategisch deshalb dem Schutz der Endsysteme verstärkte Aufmerksamkeit widmen.

7 Rechtsfragen

Mit der Installation der Software muss der Nutzer einen „Endbenutzer-Lizenzvertrag“ durch elektronische Zustimmung zu einem eingepopptem Vertragstext abschließen. Dieser Lizenzvertrag[13] (Stand 05/2013) wirft einige Rechtsfragen auf.

7.1 Zulässigkeit und Bindungswirkung

Der Lizenzvertrag wird bei der Installation in deutscher Übersetzung des englischen Originals angezeigt. Normalerweise weicht die deutsche Fassung nicht oder nur unwesentlich von der englischen ab. Hierbei ist jedoch zu beachten, dass bei Rechtsangelegenheiten die englische Fassung gilt.

Bisher wurde der Lizenzvertrag zwischen dem End User und Skype abgeschlossen. Bei einer geschäftlichen Nutzung stellt sich hier jedoch die Frage, ob der „End User“ nicht das Unternehmen ist, zumal lt. Lizenzvertrag die Rechenleistung der *eigenen* Computer und die *eigene* Bandbreite für die Skype-Community per Zustimmung zur Verfügung gestellt werden müssen.

Nach Artikel 4.1 des Lizenzvertrages wird dem Nutzer nur eine " beschränkte, nicht exklusive, nicht unterlizensierbare, nicht übertragbare, kostenlose Lizenz..." für persönliche Nutzung eingeräumt. Der Begriff "persönlich" meint dabei, dass die Lizenz sowohl nur dem Endnutzer eingeräumt wird – also *nicht* einer juristischen Person wie einem Unternehmen – als auch nur zum Zwecke der *privaten* Nutzung. Diese Formulierung wurde von Skype im Laufe der Jahre ergänzt, um Unklarheiten bzgl. einer Nutzung von Skype in Unternehmen zu beseitigen. Entsprechend wird von Skype die geschäftliche Nutzung erlaubt und unterstützt: "Es ist Ihnen erlaubt, die Software an einer Universität oder einer anderen Bildungseinrichtung oder am Arbeitsplatz zu nutzen."

7.2 Rechnernutzungserlaubnis für Skype

Gemäß Artikel 5.2 dieses Endbenutzer-Lizenzvertrags kann die Nutzung des Computers für das Skype-Netzwerk erlaubt werden: „Die Internet-Kommunikationssoftware kann die Verarbeitungsfunktionen, den Speicher und die Bandbreite des Computers (oder anderer entsprechender Geräte) nutzen, die Sie verwenden, und zwar für den beschränkten Zweck der Erleichterung der Kommunikation und der Herstellung der Verbindung zwischen den Nutzern der Internet-Kommunikationssoftware.“ Des Weiteren wird diesbezüglich auf die Nutzung von Ressourcen eingegangen, „die im Besitz einer Drittpartei stehen und von ihr kontrolliert werden“. Dies bezieht sich bspw. auf die vom Unternehmen für Mitarbeiter bereitgestellten Rechner. Für diese ist die Einwilligung zur Nutzung von Skype nach Artikel 5.2 notwendig: „Sie bestätigen und garantieren durch Akzeptieren der vorliegenden Bedingungen, dass Sie eine derartige Einwilligung eingeholt haben.“ Somit verpflichten sich Mitarbeiter bei der Nutzung von Skype auf unternehmenseigenen Rechnern zur internen Meldung und Abstimmung mit den zuständigen Verantwortlichen.

[13] Der aktuelle Lizenzvertrag ist unter http://www.skype.com/de/legal/tou/ abrufbar.

7.3 Ablehnung von Gewährleistungsansprüchen

Skype lehnt Gewährleistungsansprüche ab. Gemäß 5.4. kann es zu Ausfällen wegen Wartungsarbeiten kommen. „Sie sind nicht berechtigt, Schadenersatz für eine solche zeitweise Aufhebung oder Einschränkung der Nutzung einer Software, eines Produkts oder einer Website von Skype zu fordern."

Diese Klauseln könnten so gewertet werden, dass der Hersteller die Verwundbarkeit von Hosts und Netzwerken eingesteht. Allerdings ist es auch normal, dass sich der Hersteller einer kostenfreien Software absichert.

Das Risiko ist bei nur ergänzender Nutzung tragbar.

7.4 Löschrechte von Skype

Nach 11.2 verfügt Skype über die Möglichkeit zur zeitweiligen Aussetzung der Skype-Nutzung: „Skype kann seine Beziehung mit Ihnen beenden oder Ihre Nutzung der Software, des Nutzerkontos bzw. der Nutzerkonten, der Produkte oder der Websites von Skype jederzeit und ohne gerichtliche Anfechtbarkeit beenden oder zeitweise aufheben."

Skype behält sich somit das Recht vor, das Skype-Benutzerkonto zu löschen, „ wenn Sie gegen die vorliegenden Bedingungen verstoßen. Diese Klausel ist für einen kostenfreien Service verständlich.

Das Rechts- und Sicherheitsrisiko ist bei einer nur ergänzenden Nutzung tragbar.

7.5 Eigentum und Verwendungsrechte der Skype-ID

Im Zuge der Installation von Skype wird nicht nur ein Vertrag bezüglich der Softwarenutzung abgeschlossen, sondern auch einer bezüglich des Accounts (Skype-ID). Der bei der anschließenden Registrierung festgelegte Account ist an beliebigen Skype-Clients nutzbar.

Wird Skype für geschäftliche Aufgaben genutzt, so stellt sich die Frage, wem dieser Account gehört, wer ihn beantragen, nutzen oder löschen darf. Das Unternehmen kann dem Mitarbeiter nicht verbieten, einen privaten Skype-Account anzulegen, allenfalls es vom Unternehmens-PC aus zu tun und diesen an einem Unternehmens-Skype-Client zu nutzen. Es kann ihm auch nicht vorschreiben, seinen privat beantragten Account zu löschen, wenn sein Arbeitsvertrag ausläuft. Das geht nur bei Accounts, die die Firma besitzt.

Aus diesem Grund wird die Verwendung von zwei Skype-Accounts empfohlen – einem privaten und einem geschäftlichen Skype-Account.

Ein solches Vorgehen ist erforderlich bei Accounts, die dauerhaft als Kommunikationsadressen des Unternehmens (von Projekten, Bereichen, Funktionen) genutzt und publiziert werden, da ansonsten nicht sichergestellt werden kann, dass der Mitarbeiter den Account nach Ende seiner Tätigkeit freigibt oder löscht. Hierbei ist zu beachten, dass Skype es sich nach 11.3 vorbehält, „Nutzerkonten zu stornieren, die mehr als ein Jahr nicht aktiv waren."

8 Einsatz von Skype im Unternehmen – Policy-Empfehlung

Es ist bekannt, dass Skype von Mitarbeitern in den Unternehmen bisher genutzt wurde. Als Grund wird die Möglichkeit der verschlüsselten Kommunikation, der kostenlose Service, der Wunsch der Gesprächspartner bzw. die einfache Durchführung von Telefonkonferenzen angegeben. Ohne Softwarebeschaffung und Adminrechte können ganz einfach und kostenfrei Kommunikationsverbindungen vom Arbeitsplatz aus realisiert werden.

Durch die große, weltweite Bekanntheit und Verbreitung von Skype ist die Kommunikation mit vielen Kontakten möglich.

Skype ist daher ein – vor allem in der Projektarbeit und Kooperation von internen und externen Arbeitsgruppen – interessantes Kommunikationsmittel, das Telefon und E-Mail ergänzt. Von vorneherein nicht in Frage kommt Skype jedoch als Ersatz für herkömmliche Kommunikationsanlagen. Fehlende Leistungsmerkmale, keine Notruffunktion, fehlende Verzeichnisse und die nicht garantierbare Verfügbarkeit sprechen grundsätzlich dagegen. Es wird hier daher nur die Nutzung von Skype als Ergänzung von herkömmlicher Telefonie betrachtet.

Die Betrachtungen dieser Studie betreffen die Sprachkommunikation. Datenübertragung sollte mit Skype nicht durchgeführt werden, Chat ist mit anderen sichereren Tools möglich, Videokommunikation ist insbesondere bei interkontinentalen Verbindungen wegen Bandbreitenproblemen und Delay oft qualitativ sehr eingeschränkt und nicht empfehlenswert.

Die Nutzung von Skype wird aufgrund der in Kapitel 6 dargelegten Sicherheitsbedenken derzeit nicht empfohlen!

Es ist aktuell davon auszugehen, dass der Skype-Verkehr im Netz von den US-Nachrichtendiensten auch in Europa abgehört und aufgezeichnet wird. Daher raten wir vom Einsatz von Skype für Sprachkommunikation innerhalb Europas ab.
Für innereuropäische Sprachkommunikation sind Systeme der klassischen Telekommunikation zu bevorzugen, auch GSM erscheint hier sicherer.
Bei unternehmensinterner Kommunikation sollte möglichst die intern vorhandene TK-Infrastruktur genutzt werden. Für reisende Mitarbeiter sollten, wenn möglich, Softclients mit VPN-Zugang zu nutzen.
Außerhalb Europas ist Skype einer unverschlüsselten VoIP-Kommunikation vorzuziehen, da hier sonst noch weniger kontrollierte Nachrichtendienste die Kommunikation überwachen können.
Für vor Nachrichtendiensten sichere Telefonie mit beliebigen Partnern in der Welt, die nicht auf spezielle Endgeräte oder Endgerätesoftware angewiesen ist, gibt es derzeit keine Lösung.

Für den Austausch sicherheitsrelevanter und geschäftskritischer Informationen wird Skype und unverschlüsselte Telefonie prinzipiell nicht empfohlen!

Sollte Skype dennoch genutzt werden, ist die Installation von Skype-Software nur zulässig, wenn bestimmte Voraussetzungen erfüllt sind. Sie ist dem lokalen IT-Verantwortlichen oder IT-Sicherheitsbeauftragten zu melden, der die Voraussetzungen prüft und die Installation dokumentiert.

Dabei sind die Skype Nutzer auch über die unten aufgeführten Nutzungsregeln der empfohlenen Skype-Policy zu informieren:

a. Zulässigkeitsvoraussetzungen

- Mit dem Skype-Einsatz muss ein Nutzen für das Unternehmen verbunden sein.
- Skype ist kein Ersatz für herkömmliche Telefonie, insbesondere kein zulässiger Grund, andere Telefone ab- oder nicht neu anzuschaffen.
- Auf Rechnern sicherheitskritischer Bereiche mit einem hohen Schutzbedürfnis (Verwaltungsarbeitsplätze und -netz, Geheimschutzbereiche, etc. und auch auf Serversystemen) ist die Installation von Skype nicht zu gestatten
- Skype darf nicht auf Rechnern installiert werden, die wochen- oder auch nur tagelang durchlaufen müssen.
- Der für Skype genutzte Host (PC/Notebook) muss mit aktueller Anti-Spyware und Virenschutzsoftware ausgestattet sein.
- Dateiaustausch sollte nicht über Skype abgewickelt werden.
- Zwischen privatem und dienstlichem Account sollte unterschieden werden. Bei geschäftlichen Accounts zur gelegentlichen Nutzung sollte in den Profil-Einstellungen ein nach außen sichtbarer Bezug zur Person und zum Unternehmen vermieden werden.
- Die Nutzung kostenpflichtiger Skype-Services erfordert im Übrigen wie die aller kostenpflichtigen Services eine gesonderte Genehmigung durch die für Telekommunikationsverträge Zuständigen.
- Skype sollte in Bereichen, in denen mit sicherheitsrelevante und geschäftskritische Informationen ausgetauscht werden, nicht eingesetzt werden. Gerade bei der Kommunikation mit ausländischen Partnern sollten keine sensiblen Geschäftsdaten ausgetauscht werden.
- Skype sollte niemals bei Erstkontakt mit neuen Projektpartnern genutzt werden, sondern immer nur bei bekannten und für vertrauenswürdig erachteten Gesprächspartnern.

b. Meldung und Dokumentation

Die Skype-Installation und Nutzung ist dem lokalen IT-Verantwortlichen oder IT-Sicherheitsbeauftragten zu melden. Die Registrierungspflicht scheint bisher häufig nicht befolgt zu werden, ist aus den genannten Gründen aber zukünftig ernster zu nehmen. Dabei muss:

- eine Überprüfung der Voraussetzungen der Zulässigkeit in sicherheitskritischen Bereichen erfolgen,
- dokumentiert werden, auf welchen Geräten Skypesoftware installiert wurde und welche geschäftlichen Accounts dabei ggf. eingerichtet wurden, und
- der Benutzer über Risiken und Sicherungsmaßnahmen informiert werden.

c. Inhalte der Benutzerinformation

- Inhalt der Einsatzempfehlung und Vermittlung von Grundwissen zur Funktionsweise von Skype und dem Skype-Netz.

- Ein privat registrierter Skype-Account darf (wie andere Privatadressen auch) nicht als Standard-Kommunikationsadresse des Unternehmens (im Internet, auf Visitenkarten etc.) publiziert werden.
- Da in Skype die Identität des Rufers (Versenders von Nachrichten) nicht gewährleistet ist, sollte Skype nur zur Kommunikation mit bekannten Partnern und nicht zur Anbahnung von Geschäftskontakten genutzt werden.
- Skype-Passwörter müssen Skype-spezifisch sein und sollen nach der Verwendung eines fremden Terminals geändert werden. Für die Nutzung an fremden Terminals wird die Verwendung von Skype auf einem eigenen USB-Stick empfohlen, da in diesem Falle alle benutzerbezogenen Daten auf dem Stick gespeichert werden.
- Seien Sie wachsam: Über den Dateitransfer können verseuchte Dateien versendet werden. Sicherheitslücken in der Skype-Software sind nicht auszuschließen.
- Vertrauliches sollte nur mit vertrauenswürdigen Personen ausgetauscht werden. Durch den Gesprächspartner können Chat-Sitzungen mitprotokolliert und Gespräche mitgeschnitten werden.
- Aktivieren Sie Skype nicht automatisch (beim Start des Betriebssystems), sondern nach Bedarf. Stellen Sie Skype so ein, dass Softwareupdates nicht automatisch sondern nach Bestätigung erfolgen.
- Vermeiden Sie grundsätzlich die automatische Annahme von Verbindungen.

d. Konfiguration

- Unter Windows können einige Funktionen von Skype über Einträge in der Registry verhindert bzw. erlaubt werden. Skype stellt eine konfigurierbare MSI-Datei bereit[14]. Für Benutzer ohne Administratorrechte sind diese Vorgaben verbindlich, wenn sie als HKLM Registry keys gesetzt werden. Dies gilt selbst dann, wenn Skype von einem USB-Stick gestartet wird.
- Seit Version 3.0 unterstützt Skype die Verteilung von Einstellungen über Gruppenrichtlinien in Windows AD Umgebungen. Skype stellt hierfür eine ADM-Datei bereit[15]. Diese erlaubt es, die für Skype relevanten Registry-Einträge in einem Group Policy Object zu bestimmen, das anschließend an die zu konfigurierenden Rechner verteilt werden kann.
- Die folgenden Einstellungen in der Registry unter HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone werden empfohlen. Dadurch sollen Performance- und Bandbreitenprobleme sowie mögliche Sicherheitsrisiken vermieden werden:
  - Deaktivierung der Supernode-Funktionalität: DisableSupernode, REG_DWORD = 1
  - Deaktivierung von Dateiübertragungen: DisableFileTransfer, REG_DWORD = 1
  - Deaktivieren der API-Fähigkeit: DisableApi, REG_DWORD = 1
- Die Einstellung „Skype bei Windows-Start ausführen“ muss deaktiviert werden.
- Autologin muss deaktiviert werden.

[14] Download unter: http://www.skype.com/de/business/downloading/
[15] Download der der jeweils aktuellsten Verion über http://download.skype.com/share/business/guides/skype-it-administrators-guide.pdf

- Bitte benutzen Sie immer die aktuelle Programmversion.

9 Fazit

In Unternehmen ist Skype schon aufgrund des fehlenden Notrufs, mangelnder Verfügbarkeitsgarantien und des möglichen Zirkulierens von unternehmensinternen Kontakt- und Verbindungsdaten auf Supernodes im Internet kein Ersatz für herkömmliche Telefonanlagen.
Vorteile von Skype gegenüber SIP und herkömmlicher Telefonie liegen in der einfachen Installation und Nutzung über verschiedene Systemplattformen hinweg sowie in den genannten Leistungsmerkmalen, dort insbesondere auch die Verschlüsselung der Kommunikation. Skype bringt als freies Kommunikationsmedium jedoch zahlreiche Sicherheits- und Rechtsfragen mit sich.
Nach Meinung der Autoren sind derzeit erhebliche Sicherheitsrisiken vorhanden.

Nach einer Abwägung von Nutzen und Sicherheitsbedenken wird eine Nutzung von Skype im Unternehmen daher aktuell nicht empfohlen!

Zu diesem Schluss führten insbesondere die unter Kapitel 6.2 geschilderten Überwachungsmöglichkeiten von Verbindungs-und Kommunikationsdaten, die nach aktuellem Wissensstand auch systematisch genutzt werden.

Insbesondere für nationale Kontakte sind andere Systeme der klassischen Telekommunikation zu bevorzugen.

Bei unternehmensinterner Kommunikation sollte die interne TK-Infrastruktur genutzt werden.

Nur bei internationalen Kontakten ist Skype einer unverschlüsselten VoIP-Kommunikation vorzuziehen.

Für vor Nachrichtendiensten sichere Telefonie mit beliebigen Partnern in der Welt, die nicht auf spezielle Endgeräte oder Endgerätesoftware angewiesen ist, gibt es derzeit keine empfehlenswerte Lösung

Für den Austausch sicherheitsrelevanter und geschäftskritischer Informationen wird Skype und unverschlüsselte Telefonie prinzipiell nicht empfohlen!

Sollte man sich dennoch für eine Nutzung von Skype entscheiden, sind die in Kapitel 8 formulierten Handlungsempfehlungen bezüglich:
- Zulässigkeitsvoraussetzungen
- Meldung und Dokumentation
- Inhalte der Benutzerinformation
- Konfiguration

zu beachten.

Literaturverzeichnis

Baset, S. A., & Schulzrinne, H. (2004). *An Analysis of the Skype Peer-to-Peer Internet Telephony.* New York.

Biondi, P., & Desclaux, F. (2006). *Silver Needle in the Skype.* Suresnes.

BSI. (2005). *VoIPSEC - Studie zur Sicherheit von Voice over Internet Protocol.* Bonn.

Desclaux, F. (2005). *Skype uncovered - Security study of Skype.*