IT Security and Service Management
Steinbuch Centre for Computing
Karlsruhe Institute of Technology

# Sicherheitsgutachten »skype«

Dipl.-Inform. Adrian Wiedemann Dipl.-Inform. Tobias Dussa

7. Oktober 2008

[adrian.wiedemann,tobias.dussa]@kit.edu

Das vorliegende Dokument begutachtet die Software »skype« der Firma Skype Technologies SA im Hinblick auf den Einsatz als Kommunikationssystem innerhalb des KIT. Bei dieser Betrachtung wird eine Risikoeinschätzung beim Einsatz als Kommunikationsplattform gegeben, eine Begutachtung im Sinne einer Fehleranalyse der konkreten Implementation kann nicht geleistet werden. Ziel des Gutachtens ist, eine sicherheitstechnische Betrachtung der verwendeten Software durchzuführen und eine Risioabschätzung des Einsatzes der Software zu geben.

## 1 Beschreibung der begutachteten Software

Die Software »skype« wird von der Firma Skype Technologies SA mit Sitz in Luxemburg hergestellt und vertrieben. Skype Technologies SA selbst ist eine 100%tige Tochter der Firma eBay Corp. Mittels der von Skype Technologies SA vertriebenen Software ist es möglich, mit anderen Personen, die diese Software verwenden, über das Internet zu kommunizieren. Die Software ist für die Verwendung dabei auf den entsprechenden (Computer-)Endgeräten zu installieren, aktuell werden die gängigsten Betriebssysteme unterstützt.

Für die Benutzung der Software wird diese dem Benutzer in einen Binärformat zur Verfügung gestellt, ein Einblick in den Quelltext des verwendeten Programms ist nicht möglich. Die Disassemblierung der Software wird durch kryptographische Mechanismen verhindert, aus diesem Grund kann auch keine Begutachtung des Binärprogramms durchgeführt werden.

## 2 Beschreibung der Kommunikationsressourcen

Für eine erfolgreiche Verwendung der Software ist das Vorhandensein bestimmter Ressourcen der Firma Skype Technologies SA selbst aus verschiedenen Gründen notwendig. Skype Technologies SA betreibt Server, die für den Aufbau des Kommunikationskanals notwendig sind. Die Anzahl der Server und deren Aufstellungsort(e) sind nicht bekannt. Des weiteren betreibt Skype Technologies SA Server, die für das Dienstmerkmal »Skype-out« notwendig sind. Bei Nutzung dieses Dienstmerkmals wird eine Kommunikationsverbindung zwischen der »skype«-Software und Teilnehmern in einem externen Kommunikationsnetz, beispielsweise dem der Deutschen Telekom, hergestellt.

Es sind folgende Komponenten bei Nutzung der Software »skype« beteiligt:

- »skype«-Zentralserver
- »skype«-Gateways in externe Telefonnetze (Skype-out gateways)
- Endgeräte mit »skype«-Software

Die Kommunikation zwischen zwei »skype«-Teilnehmnern verwendet in den Phasen des Kanalauf- und abbaus sowie der Kanaländerung die Server von Skype Technologies SA; die Kommunikation selbst erfolgt direkt zwischen den Teilnehmern. Im Fall der Verwendung des Dienstmerkmals Skype-out wird als »skype«-seitiger Endpunkt eines der Skype-out gateways verwendet. Eine weitere Vermittlung kann von Skype Technologies SA nicht beeinflusst werden und obliegt dem am Skype-out gateway angeschlossenen Provider.

## 3 Risiken

Aus Sicht der Anwender bestehen bei Verwendung der Software »skype« zwei wesentliche Risiken:

- Abhören der Kommunikation über »skype«. Die Gefahr des Abhörens der Kommunikation mit »skype« ist nicht nur für die Sprachkommunikation, sondern für alle von Skype angebotenen Kommunikationskanäle relevant. Die Gefahr des Abhörens ist nicht nur bei der Nutzung von »skype« innerhalb einer Einrichtung gegeben, sondern insbesondere auch bei externen Veranstaltungen, bei denen die Absicherung des direkten Zugangs nicht den Sicherheitsanforderungen der Einrichtung entspricht.
- Angreifbarkeit der Endsysteme über »skype«. Endsysteme können über die Kommunikationskanäle von »skype« in der Weise angegriffen werden, dass ein Fehler in der Programmierung der Software Manipulationen am System oder das Ausspähen von Daten auf diesem System erlaubt. Falls dieser Angriffsvektor ausgenutzt wird, sind grundsätzlich alle Systeme, auf denen die verwundbare Implementation von »skype« installiert ist, angreifbar.

Aus Sicht des Betreibers einer Infrastruktur birgt die Nutzung von »skype« folgende Risiken:

- Unterwanderung von Sicherheitsperimetern. Betreiber von größeren Infrastukturen haben im Regelfall verschiedene Zonen mit unterschiedlichen Sicherheitseinstufungen aufgebaut, die dem Zweck dienen, den Zugriff von außerhalb des Perimeters zu verhindern. Durch die Nutzung von »skype« können diese Sicherheitsperimeter aber umgangen werden, da in den allermeisten Fällen nur der Verbindungsaufbau, nicht aber die eigentliche Übertragung verhindert wird.
- Bei der Verwendung von »skype« ist ein weiteres Merkmal beim Aufbau der Kommunikationskanäle zu beachten. Die Software »skype« ermittelt die Bandbreite des Endsystems und kann gegebenenfalls als sogenannter Supernode zusätzlich Aufgaben übernehmen, die für die Vermittlung von Kommunikationskanälen notwendig sind.

## 4 Bewertung

Die genannten Risiken entstehen durch versehentlich fehlerhafte oder absichtlich schädliche Software. Es stellen sich damit für den Benutzer die folgenden Fragen:

1. Kann meine »skype«-Kommunikation abgehört werden?
2. Ist mein Endgerät, auf dem die »skype«-Software installiert ist, angreifbar?

Für die Betreiber von Infrastrukturen sind folgende Fragestellungen beim Einsatz von »skype« relevant:

1. Kann die Verwendung von »skype« mein Sicherheitsperimeter unterlaufen und vorhandende Maßnahmen zur Verbesserung der Endbenutzersicherheit aushebeln?
2. Kann beeinflusst werden, ob meine Infrastruktur für die Vermittlung von »skype« Kommunikationskanälen verwendet wird?

Aufgrund der verschlüsselten Verteilung der Software ist keine Prüfung der in der Software verwendeten kryptographischen Verfahren möglich. Die Analyse der Datenpakete hat ergeben, dass nach einer initialen Verbindungsaufbauphase sämtliche Datenkommunikation verschlüsselt wird.

Skype Technologies SA selbst gibt an, dass für die Verschlüsselung des Datenstroms und die Authentifizierung der Nutzer sowohl symmetrische als auch asymmetrische Verfahren verwendet. Skype Technologies SA hat ein Gutachten in Auftrag gegeben, das die in der Software eingesetzten kryptographischen Subsysteme begutachtet. Dieses Gutachten ist frei verfügbar.[3]

Rechnersysteme, auf denen »skype« installiert ist, haben allein durch die Installation des Softwarepaketes einen größere Angriffsfläche als Systeme ohne

»skype«. Aufgrund der intensiven Nutzung von kryptographischen Verfahren, die laut Aussage von Skype Technologies SA auch Veränderungen am Programmcode erkennen, kann davon ausgegangen werden, dass die »skype«-Software nach der Installation auf dem Rechnersystem des Nutzers nicht manipuliert werden kann, ohne dass der Nutzer Kenntnis davon erlangt. Dies schließt aber die Möglichkeit nicht aus, dass von Anfang an eine programmtechnische Hintertür in »skype« vorhanden ist, die gegebenenfalls aktiviert werden kann. Trotz allem gab es in der Vergangenheit Angriffe auf »skype«: Auf der Sicherheitskonferent Black Hat in Amsterdam 2006 gab es einen Vortrag über mögliche Angriffe auf »skype«.[1].

Sicherheitsperimeter wie Paketfilter können durch »skype« ausgehebelt oder umgangen werden. Dabei verwendet »skype« aber keine unbekannten Mechanismen, sondern nutzt die Tatsache aus, dass für die Kommunikation zwischen Endgeräten eine durchgängige Verbindung aufgebaut werden muss. Der Port, der für die Erreichbarkeit des Endsystems nach außen geöffnet wird, kann dynamisch sein oder fest eingestellt werden. »skype« kann des weiteren auch die festen TCP-Ports 80 oder 443 für den eingehenden Datenstrom verwenden; dies ist aber nur eine Option.

»skype« verwendet die TCP-Subsysteme des entsprechenden Betriebssystems, es können die Sicherheitsmechanismen, die für die Absicherung des Rechners verwendet werden, eingesetzt werden. Zusätzlich bietet »skype« eine Schnittstelle für Antivirenprogramme an, um Daten, die über die verschlüsselten Verbindungen auf das Endsystem gelangen, auf schadhaften Inhalt zu überprüfen.

Ab der Version 3.0 bietet »skype« an, die Möglichkeit, als Supernode aufzutreten, zu deaktiveren. Wenn diese Funktion abgeschaltet ist, werden Gespräche nicht mehr über diese »skype«-Instanz vermittelt.

Falls »skype« im größeren Maßstab auf Windows-Plattformen verteilt wird, kann über eine administrative Vorlage für Gruppenrichtlinien sichergestellt werden, dass die »skype«-Konfigurationen aller Rechner, die durch diese Richtlinie gesteuert werden, identisch sind.

# 5 Empfehlung

Skype Technologies SA stellt mit der Kommunikationssoftware »skype« eine Möglichkeit dar, schnell und unkompliziert über das Internet zu kommunizieren. Eine grundsätzliche Unbedenklichkeit der Software kann nicht bescheinigt werden, da es bereits erfolgreiche Angriffe auf »skype« gegeben hat. Auch das von der Firma Skype Technologies SA in Auftrag gebenene Gutachten aus dem Jahre 2005 kann nur als Hinweis auf die Sicherheit der Software verstanden werden.

Der Gefahr, aufgrund der Vermittlungsfunktionalität als Provider verstanden zu werden, kann durch die Deaktivierung dieser Funktionalität begegnet

werden.

Falls die Verwendung von »skype« in größerem Maßstab erlaubt oder gefördert werden soll, ist für das KIT eine Richtlinie zu erlassen, die die Randbedingungen für den Einsatz genau definiert. Diese sollte folgende Punkte beinhalten:

- Definition des Kommunikationsports nach außen.
- Verpflichtung zur Deaktivierung der Vermittlungsfunktionalität (Supernode).
- Verpflichtung zur Anbindung an zentrale Verzeichnisdienste wie Active Directory, falls möglich.
- Verweis auf die Sicherheitshinweise von Skype Technologies SA[2]

Grundsätzlich muss beim Einsatz innerhalb des KIT darauf geachtet werden, in welchem Umfeld die Software eingesetzt wird. Für die Verwendung auf Arbeitsstationen von Mitarbeitern, auf welchen per se keine sensiblen Daten verarbeitet werden, ist die Verwendung unter den für das KIT definierten Regeln als nicht besonders kritisch zu betrachten. Rechner, die für die explizite Verarbeitung von personenbezogenen Daten, betriebswirtschaflichen Daten des KIT, prüfungsrelevanten Daten des Lehrbetriebs oder anderen besonders schützenswerten Daten verwendet werden, sollten keine andere Software als die für den beabsichtigen Zweck installiert haben. In den oben erwähnten Beispielen schließt dies die Installation und Nutzung von »skype« oder anderer Software ähnlicher Funktionalität aus.

Bei Rechnersystemen von leitenden Angestellen ist im Einzelfall zu entscheiden, ob die Nutzung von »skype« notwendig ist oder ob nicht auf andere (eventuell nicht-rechnergebundene) Verfahren für audio-visuelle Kommunikation zurückgegriffen werden kann.

Zusätzlich sollten Verhaltensregeln, wie sie auch im Bereich Videoconferencing Anwendung finden, definiert und umgesetzt werden. Hierzu gehört beispielsweise das Abschalten des Mikrofons oder das Abmelden von »skype«, wenn der Rechner über eine längere Zeit verlassen wird.

## Literatur


[1] `http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-biondi/bh-eu-06-biondi-up.pdf`

[2] `http://www.skype.com/security/`

[3] `http://www.skype.com/security/files/2005-031%20security%20evaluation.pdf`