

Fachhochschule München
Fachbereich 07 Informatik/Mathematik



Praktikum Datenschutz und Datensicherheit
Sommersemester 2007

Prof. Dr. Rainer W. Gerling
Heidi Schuster

Skype im Unternehmen

Patricia Berger
IBB6A

Rony Degen
IBB6A

28.07.2007

Inhaltsverzeichnis

INHALTSVERZEICHNIS	II
GRUNDLAGEN VON SKYPE	1
WAS IST SKYPE?	1
ENTSTEHUNGSGESCHICHTE.....	1
ARCHITEKTUR DES SKYPE-NETZWERKS	2
UMGANG MIT FIREWALLS	3
DIE RICHTIGE HARDWARE	4
SICHERHEIT DER DURCH SKYPE ÜBERTRAGENEN DATEN	4
VERSCHLÜSSELUNG	4
ANGREIFBARE AUTHENTIZITÄT.....	6
GEFAHREN DURCH DIE SKYPE – SOFTWARE	6
CLOSED-CODE UND DIE FOLGEN.....	6
GEFÄHRDUNG DES UNTERNEHMENSNETZES UND WIRTSRECHNERS.....	7
VIREN, WÜRMER UND TROJANER	7
BELASTUNG DES NETZES	8
SKYPE UNTER KONTROLLE BRINGEN ODER LOSWERDEN, WENN ES SEIN MUSS.....	9
DER FAKTOR MENSCH	10
DER BENUTZER LIEBT SKYPE, DAS UNTERNEHMEN MANCHMAL AUCH.....	10
UMGANG MIT UNTERNEHMENSKRITISCHEN DATEN	10
SOCIAL HACKING.....	11
SKYPE AUF DEM USB-STICK.....	12
EMPFEHLUNG UND FAZIT	12
LITERATURVERZEICHNIS	13

Grundlagen von Skype

Was ist Skype?

Skype ist eine kostenlose Voice-over-IP (VoIP) Software, welche es primär erlaubt verschlüsselte Telefonate über das Internet zu führen. Neben dieser Haupteigenschaft beherbergt Skype zum aktuellen Zeitpunkt der Version 3.x noch folgende Dienste:

- Konferenzgespräche mit bis zu 10 Teilnehmern
- Rufaufbau zu klassischen Festnetz- oder Handytelefonen (SkypeOut)
- Rufannahme von zu klassischen Festnetz- oder Handytelefonen (SkypeIn)
- SMS-Versand an Mobiltelefone
- Videotelefonie
- Chat-Funktionalität Gruppen von bis zu 48 Teilnehmern
- Plattformübergreifender Dateiübertragung
- Und weitere ...

Die Software ist portiert für die Betriebssysteme:

Windows XP, Windows 2000, Linux, Mac OS X und Pocket PCs, die mit Windows Mobile betrieben werden [1 S. S. 5].

In der Standardversion sind bei Windows keine Administrationsrechte zur Installation nötig.

Seit der Version 3.x steht eine erweiterte Business Version unter

<http://www.skype.com/intl/de/business/> zur Verfügung, allerdings vorerst nur für Windows Betriebssysteme.

Besonders die IT-Administratoren werden sich über ein Windows MSI Installer-Paket¹, über das man Skype Business im Unternehmen über eine Netzwerkinstallation zentral bereitstellen kann, freuen. Es lassen sich wichtige Schlüsselfunktionen dieser Version durch den Einsatz verschiedenster Einstellmöglichkeiten, sei es durch die Registry-Einträge, XML basierte Konfigurationsfiles oder windowsbasierten Gruppenrichtlinien weitgehendstes steuern. Beispielsweise lässt sich dadurch die kritisch zu betrachtende Funktionalität der Dateiübertragung abschalten [1 S. 33 - 37].

Zusätzlich wird von Skype eine Verwaltungssoftware zur Verfügung gestellt, die u.a. Guthaben und Rufnummern für SkypeIn und SkypeOut administriert.

Entstehungsgeschichte

Die erste brauchbare VoIP-Software wurde 1995 von der israelischen Firma „VocalTec“ veröffentlicht. Nach einem kurzzeitig hohen Medienecho verschwand die Technologie allerdings wieder. Die Gründe lagen in der zu geringen Bandbreite des Internets, unausgereifter Software und serverbasierter Infrastruktur. Besonders der letzte Punkt machte diesen zentralisierten Ansatz durch den hohen Serverbedarf bei steigender Nutzerzahl kostenintensiv. Es dauerte über sieben Jahre bis wieder ein Unternehmerteam die VoIP-Bühne betrat, um von sich reden zu machen. In der Absicht der Telefonbranche ernsthaft Konkurrenz zu machen, veröffentlichten die Entwickler des Filesharing-Netzwerks „KaZaa“ Niklas Zennstrom und Janus Friis am 29 August 2003 eine erste Beta-Version von „Skype“. Diese Software bügelte die Nachteile der bis dahin entwickelten VoIP-Lösungen aus, was in erster Linie der Erfahrung der beiden Entwickler zu verdanken ist [2 S. 1].

¹ Administratoren haben dabei die Möglichkeit, ein vorhandenes MSI-Paket durch eine MST (Transform-Datei) zu verändern, um die zu verteilende Software individuell auf die Benutzer(gruppen) anzupassen.

Architektur des Skype-Netzwerks

Das Skype Netzwerk basiert auf einem proprietären² VoIP-Protokoll, das auf eine dezentrale Peer-to-Peer³ Netzwerkarchitektur aufsetzt. Dadurch werden die Kosten der Infrastruktur größtenteils durch die Benutzer selbst getragen, was die Kosten für „Skype“ selbst niedrig hält. Diese Netzwerkinfrastruktur besteht aus vier Kernkomponenten, die nun einer näheren Betrachtung unterzogen werden.

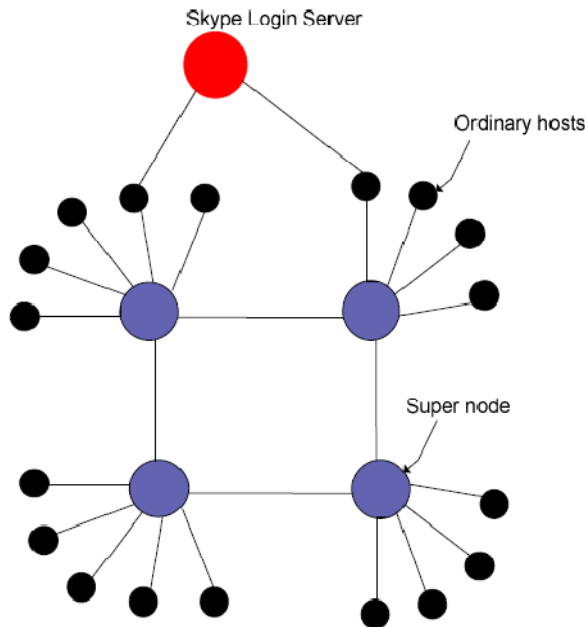


Abbildung 1: Aufbau des Skype-Netzwerks [3 S. 4]

- **Ordinary hosts:** Sie sind die Endpunkte des Netzwerks und stellen einen Standardnutzer bzw. Client dar.
- **Super nodes:** Jeder Client hält Verbindung mit mindestens einem „super node“. Dieser übernimmt spezielle Verwaltungsaufgaben. Er hält u.a. Informationen über Anrufsignalisierung, Erreichbarkeit seiner angeschlossenen Hosts vor. Außerdem verwaltet er eine Liste aller erreichbaren „super nodes“ im Netzwerk sog. „host-cache“. Sie übernehmen damit eine Vermittlerrolle.
- **Login Server:** Beim Start des Clients registriert und authentifiziert sich dieser bei einer zentralen Stelle im Netz, dem sog. „Login Server“. Desweiteren werden Informationen über erreichbare super nodes und Update-Informationen ausgetauscht.
- **Relay:** Sollte eine direkte Verbindung zweier Clients aus technischen Gründen nicht möglich sein, hilft ein Client oder super node bei der Weiterleitung des Datenverkehrs. Doch diesen Aspekt gilt es an anderer Stelle näher zu betrachten.

Bemerkenswert ist, dass ein und dieselbe Software alle aufgezählten Funktionen, mit Ausnahme derer des Login Server beinhaltet. Diese kann bei Bedarf und unter definierten Umständen, die geschilderten Rollen einnehmen.

² hier im Sinne von: kein allgemeiner Standard, eine „hauseigene“ Entwicklung, die nicht offen liegt.

³ In einem Peer-to-Peer-Netz sind alle Computer gleichberechtigt und können sowohl Dienste in Anspruch nehmen als auch Dienste zur Verfügung stellen.

Umgang mit Firewalls

Skype steht im Ruf Firewalls relativ leicht überwinden zu können und tatsächlich hat Skype einige Möglichkeiten auch hinter einer Firewall Verbindungen aufzubauen.

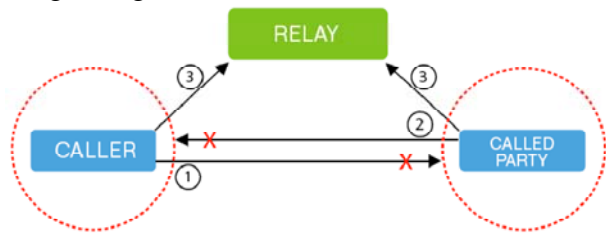


Abbildung 2: Verbindungsaufbau [3 S. 5]

Grundsätzlich versucht Skype bei einem Verbindungsaufbau zunächst eine direkte Verbindung ① aufzubauen. Hierfür fordert Skype die notwendige Information (IP-Adresse⁴, Port⁵, u.ä.) vom super node ③ an, der diese vorhält oder in einem hierarchischen Indexsystem selbst bei anderen super nodes recherchieren muss.

Die Aufgabe von Firewalls ist primär Versuche unaufgeforderter Verbindungen von außen nach innen zu verhindern, indem sie die Ports für eingehenden Verkehr sperrt, um z.B. ein Unternehmensnetz vor Angriffen von außen zu schützen. Falls ein Rechner jedoch von innen heraus die Öffnung eines Ports fordert, sind die meisten Firewalls so eingestellt dieser Anforderung zu entsprechen.

Hier setzt Skype an. Befindet sich der angerufene Skype Client hinter einer Firewall ①, bekommt dieser die Versuche des Verbindungsaufbaus nicht mit. Also werden über den super node ③ die „geschützten“ Skypeclients ② dazu veranlasst die Ports zum Verbindungsaufbau von innen bei der Firewall anzufordern, die diese dann öffnet. Folglich können nun wieder direkt Daten ausgetauscht werden [3 S. 5]. Diese Methode des Verbindungsaufbaus wird in der Fachwelt häufig auch mit den Stichworten „UPD hole punching“ und „STUN Protocol“ in Verbindung gebracht.

Ist nun aufgrund restriktiverer Firewall-Einstellungen eine Öffnung der Ports von innen nicht möglich, sind die Optionen der Kommunikation noch nicht ausgeschöpft. Das liegt zum Einen an der Tatsache, dass jeder Client mehrere Mechanismen des Verbindungsaufbaus z.B. automatische Proxy-Server zu erkennen bzw. auf den Port 80 (http-Dienst) oder Port 443 (https-Dienst) zurückzugreifen hat. Die Ports sind grundsätzlich offen, da sonst kein „Surfen“ im Internet möglich ist. Zum Anderen kann ein super node oder anderer Client auch als Weiterleiter sog. Relay ③ zwischen zwei Clients in Erscheinung treten, die sonst nicht direkt miteinander kommunizieren könnten. Zwar sind dadurch eventuell Sprachqualität und/oder Übertragungsleistung eingeschränkt, aber dennoch möglich.

Scheinbar gibt es auch eine ähnliche Funktion, falls die IP Adressen der Skype Login-Server gesperrt werden. Es steht zu vermuten, dass in diesem Fall ein Super-Node als Login-Vermittler fungiert.

Es ist allerdings zu vermuten, dass noch weitere Methoden bestehen Firewalls zu überwinden.

⁴ Eine IP-Adressen (Internet-Protokoll-Adresse) ist eine innerhalb eines Netzwerks eindeutige Nummer unter der Rechner und andere dem Netz angeschlossene Geräte (Router, Access Points, usw.) identifiziert werden können.

⁵ Ports sind Adresskomponenten, die in Netzwerkprotokollen eingesetzt werden, um Datensegmente den richtigen Diensten zuzuordnen, z.B. wird über Port 80 (es gibt diese von 0 bis 65535) der http-Dienst angeboten.

Die richtige Hardware

Sollte es trotzdem notwendig sein, Skype auf Netzwerkebene neutralisieren zu müssen, bleibt zu sagen, dass dies mit „billigen“ NAT⁶ / Port-basierten Firewalls ein schwieriges Unterfangen ist. Einige Anbieter von Netzwerkkomponenten wie Verso, Ipoque, Lynanda, SonicWall, Packeteer und andere können dies jedoch bewerkstelligen. Deren Verfahren basieren in der Regel auf Analyse der Protokolle und Datenpakete. Diese werden nach Skype-spezifischen Mustern durchsucht und bei Bedarf wird dann der entsprechende Netzwerkverkehr blockiert. Selbst der beliebte, skalierbare und kostenlose Proxy-Server⁷ „Squid“ kann mit den entsprechenden Anpassungen Skype blockieren [4]. Der Ansatz hier ist vergleichsweise simpel, aber sehr wirkungsvoll. „Squid“ wird durch Filter veranlasst, IP-Adressen nicht direkt aufzurufen. Auf das Surfen oder den Email-Verkehr hat das praktisch keinen Einfluss, da hier zuerst die Domainnamen (www.beispiel.de; email@beispiel.de) in IP-Adressen (indirekt) umgesetzt werden. Skype, das auf die direkte Vermittlung per IP-Adressen angewiesen ist, hingegen wird „trockengelegt“.

Sicherheit der durch Skype übertragenen Daten

Verschlüsselung

Wie bereits dargestellt, kommen zwangsläufig weitere Rechner mit Signalisierungs- oder Kommunikationsdaten (Relays, super nodes, Proxy-Server) in Berührung. Es wäre technisch kein großer Aufwand an diesen Stellen gesuchte Daten abzugreifen, was allerdings in den meisten Fällen zumindest aus Nutzersicht nicht erwünscht ist.

So kam Skype zu dem Schluss, dass nur eine starke Endpunkt-zu-Endpunkt Verschlüsselung das Problem lösen kann. Auf diese Weise können alle Rechner, die als Zwischenstationen dienen, kein Teil der Kommunikation werden, sondern sind nur ein neutraler Teil der Leitung.

Diese Verschlüsselung wird prinzipiell wie folgend beschrieben initialisiert. Zunächst wird nun die Anmeldung an das Skype-Netzwerk betrachtet:

1. Versucht der Skype-Nutzer sich am Skype-Netzwerk anzumelden, errechnet sein Skype-Client ein RSA⁸ Schlüsselpaar (Privater und öffentlicher Schlüssel) und einen Hashwert⁹ des Passwortes.
2. Der Client verbindet sich dann per AES¹⁰ Verschlüsselung mit dem zentralen Login-Server und prüft, ob es sich dabei wirklich um den richtigen Server handelt.
3. Danach sendet der Client Benutzername, Hashwert des Passwortes und seinen öffentlichen Schlüssel an den Login-Server.

⁶ NAT (Network Address Translation) ist der Sammelbegriff für Verfahren, um Adressinformationen (IPs, Ports) in Datenpaketen durch andere zu ersetzen, z.B. zwischen externen Internet und internen Unternehmensnetz.

⁷ Proxy-Server können verschiedene Aufgaben übernehmen, wie z.B. Zwischenspeicherung häufig benutzter Webinhalte um damit Verringerung der Netzbelastung, Zugriffssteuerung, Inhaltsfilterung und vieles mehr.

⁸ RSA ist ein asymmetrisches Verschlüsselungssystem, das sowohl zur Verschlüsselung als auch zur digitalen Signatur verwendet werden kann. Es verwendet ein Schlüsselpaar bestehend aus einem privaten Schlüssel, der zum Entschlüsseln oder Signieren von Daten verwendet wird, und einem öffentlichen Schlüssel, mit dem man verschlüsselt oder Signaturen prüft.

⁹ Ein Hashwert wird auch als Fingerprint (Fingerabdruck) bezeichnet. Denn wie ein Fingerabdruck einen Menschen nahezu eindeutig identifiziert, ist ein Hashwert eine eindeutige Kennzeichnung eines digitalen Ausdrucks z.B. von Dateien, Passwörtern oder ähnlichem.

¹⁰ Der Advanced Encryption Standard (AES) ist ein symmetrisches Verschlüsselungssystem. Nach seinen Entwicklern Joan Daemen und Vincent Rijmen wird er auch Rijndael-Algorithmus genannt (gesprochen wie dt. „Reyndahl“).

4. Ist alles in Ordnung empfängt der Client ein 1.539 oder 2.048 Bit RSA Identitätszertifikat vom Server entsprechend seines Benutzernamens.

Damit steht eine sichere Verbindung zum Skype Netzwerk. Weiter geht es mit der Verschlüsselung zwischen zwei Clients zum Austausch von Daten:

1. Versucht nun ein Client einen anderen zu kontaktieren, tauschen beide Seiten ihre zuvor erhaltenen Identitätszertifikate aus und prüfen jeweils deren Echtheit.
2. Danach erzeugt jeder der beiden Clients für sich zufällige 128 Bit-Schlüssel und tauscht diesen per RSA-Verschlüsselung mit seinem Partner aus.
3. Somit erhält jeder einen insgesamt 256 Bit-Sitzungsschlüssel, der die Kommunikation der beiden Clients ab sofort schützt.

Es ist zu erwähnen, dass dieser Schlüssel nur solange gültig ist, wie diese Sitzung anhält. Jede weitere Sitzung erhält wieder einen neuen Schlüssel.

Ab dem Zeitpunkt der Verschlüsselung der Sitzung werden alle Daten, sei es Sprache, Chat oder Dateitransfer verschlüsselt. Wie sicher die Daten letztendlich sind, kann nicht endgültig beantwortet werden. Skype gibt kaum Details dazu preis. Allerdings wurde im Jahr 2005 der anerkannte Verschlüsselungsexperte Tom Berson mit der Überprüfung des Skype-Systems beauftragt, der es als sicher „beschrieb“ [5]. Es gibt aber auch kritische Stimmen, die zumindest die bisher theoretische Möglichkeit aufzeigen, manipulierte super nodes einzuschleusen und auf diese Weise den Datenstrom umzuleiten. Wer sich mit dieser Thematik auf sehr technischem Niveau weiter befassen möchte, sollte sich dazu die Arbeiten von Philippe Biondi und Fabrice Desclaux, beide Mitarbeiter der EADS, näher anschauen, welche zahlreich bei Google unter deren Namen zu finden sind. Stichwörter sind in diesem Zusammenhang auch „Vanilla Skype 1¹¹ und 2¹²“, „Silver Needle in the Skype¹³“, „Skype uncovered¹⁴“ oder „Castle in the Skype¹⁵“. Auch ein Report mit dem Titel „An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol¹⁶“ der Universität Columbia, der bereits im Jahre 2004 veröffentlicht wurde, bringt weiteren Aufschluss.

Sicher sind Gespräche demnach nur innerhalb des Netzwerkverbundes von Skype, das heißt folglich, wenn SkypeIn bzw. SkypeOut benutzt wird, ist das Abhören ab dem Punkt möglich, wo der Datenstrom entschlüsselt werden muss, um als Akustik in das öffentliche Telefonnetz eingespeist zu werden. Auch andere Ansätze ähnlicher Art sind möglich, beispielsweise das Anzapfen der Soundkartentreiber eines Rechners, denn schließlich muss auch hier der Datenstrom wieder in Akustik verwandelt werden.

Regierungen, Ermittlungseinrichtungen und professionelle „Datenbesorger“ werden sich nicht ewig aussperren lassen. Man kann sicher sein, dass hier Druck ausgeübt wird, wie auch Professor Andreas Pfitzmann, Leiter der Datenschutz- und Sicherheitsgruppe der Technischen Universität Dresden, vermutet [6]. Sicherheit ist in der Informatik manchmal ein eher temporäres Phänomen.

¹¹ Siehe <http://recon.cx/en/f/vskype-part1.pdf>

¹² Siehe <http://recon.cx/en/f/vskype-part2.pdf>

¹³ Siehe <http://blackhat.com/presentations/bh-europe-06/bh-eu-06-biondi/bh-eu-06-biondi-up.pdf>

¹⁴ Siehe http://www.ossir.org/windows/supports/2005/2005-11-07/EADS-CCR_Fabrice_Skype.pdf

¹⁵ Siehe <http://actes.sstic.org/SSTIC06/Castle in the Skype/SSTIC06-Desclaux-Castle in the Skype.pdf>

¹⁶ Siehe <http://www1.cs.columbia.edu/~library/TR-repository/reports/reports-2004/cucs-039-04.pdf>

angreifbare Authentizität

Wikipedia beschreibt Authentizität in der Informatik als die sichere Zuordnung einer Information zum Sender und der Nachweis, dass die Informationen nach dem Versand nicht mehr verändert worden sind.

Gedankenspiel 1:

Sie treffen Ihren Geschäftskontakt „Peter Beispiel“. Unterhalten sich, stellen eine Gemeinsamkeit fest. Sie haben beide Skype. Er sagt, er rufe Sie per Skype gelegentlich mal durch. Skype-Namen werden nicht ausgetauscht. Tatsächlich, ein paar Tage später bittet der Skype-Name „PeterB“ um Aufnahme in die Ihre Kontaktliste und sendet Ihnen auf gleichem Wege eine Datei mit dem Titel „willkommen.exe“. Sie, nicht auf den Kopf gefallen, sehen in seinem Profil bei Skype nach, wie seine Profildaten sind und es scheint alles zu passen. Ist damit „Peter Beispiel“ authentifiziert? Nein! Denn wenn man sich bei Skype erstmalig registriert ist keine Überprüfung der angegebenen Daten (Name, Wohnort, etc.) vorgesehen. Somit ist auch möglich Identitäten vorzugaukeln. Natürlich sind auch die Kommunikationstypen von Skype unterschiedlich zu bewerten. Bei einem Videoanruf lässt sich eine gefälschte Identität sicher bei weitem schlechter vortäuschen als bei einem Chatgespräch.

Gedankenspiel 2:

Wie oben, allerdings tauschen Sie beide nun Ihre Skype-Namen aus. Sie wissen nun, dass es sich tatsächlich um die besagte Person handelt. Sprechen und Chatten (keine Videotelefonie) mit ihr ein paar Mal im Monat per Skype. Eines Tages geht das Chatfenster auf und Sie werden gefragt wie den das Geschäft so laufe. Ist jetzt endlich „Peter Beispiel“ authentifiziert? Nein! „Peter Beispiel“ könnte seinen Laptop verloren haben, Skype-Passwort war eingespeichert. Ab sofort kann sich der Finder als „Peter Beispiel“ ausgeben. Oder jemand sieht „Peter Beispiel“ beim Eintippen seines Passworts zu. Oder „Peter Beispiel“ ist in die Pause gegangen und hat seinen Rechner nicht gesichert. Oder ein Virus spielt die Kommunikation nur vor. Es gibt sicher noch weitere Szenarien.

Summiert man diese Erkenntnisse mit der theoretisch angesprochenen Möglichkeit super nodes zu manipulieren, muss schon allein aufgrund des Vorsichtsprinzips davon ausgegangen werden, dass je nach verwendeter Kommunikationsart die Authentizität angreifbar und im Zweifelsfall nicht gegeben ist.

Gefahren durch die Skype – Software

Closed-Code und die Folgen

Im Gegensatz zu open code software, bei welcher der Quellcode des Programms offenliegt und somit begutachtet werden kann, ist Skype closed code. Das heißt niemand, außer einiger Eingeweihter von Skype, kennt alle Funktionalitäten der Software. Somit vertritt Skype das Prinzip von „Security through Obscurity“ sowohl beim verwendeten Protokoll als auch bei der zugehörigen Software. Mehr noch, die Software entzieht sich bisher konsequent allen Versuchen des Re-Engineerings, beispielsweise durch Erkennung derartiger Re-Engineering-Tools im Speicher und anschließender Änderung des Laufzeitverhaltens.

Es gibt somit die theoretische aber ernst zu nehmende Möglichkeit nicht dokumentierter Funktionen, mit deren Hilfe der Wirtsrechner überwacht, ferngesteuert oder gezielt ausspioniert werden könnte. Mit einem derartigen „Brückenkopf“ ließe sich auch das restliche Netzwerk weiter „erforschen“. Einige Kritiker, wie die angesprochenen EADS Mitarbeiter, gehen noch weiter und bezeichnen Skype als größtes „Bot-Net“.

Gefährdung des Unternehmensnetzes und Wirtsrechners

Aber auch wenn eventuell nicht dokumentierte Funktionen außen vor gelassen werden, kann von der Software an sich Gefahr in Form von gezielten Manipulationen Dritter ausgehen, die ebenfalls die oben genannten Gefahren in sich bergen. Eine gemeinsame Studie von InfoWatch und dem russischen Online-Portal SecurityLab.ru ist diesem Szenario mit folgendem Ergebnis weiter nachgegangen:

Datum	Schwachstelle
November 2004	Die entdeckte Schwachstelle ermöglichte einem Hacker, die vollständige Kontrolle über einen Anwender-PC per Buffer-Overflow in Skype zu erhalten.
April 2005	Skype schloss die Zugangsrechte nicht immer akkurat. Ein Hacker hat so mit der bereits empfangenen Authentifizierung Originalanwendungen durch modifizierte ausgetauscht.
Oktober 2005	Über ein Schlupfloch hat ein Übeltäter per Buffer-Overflow Zugang zum System erhalten.
Oktober 2005	Eine Lücke in Skype ermöglichte eine Remote-Attacke auf einen Computer.
Mai 2006	Eine neue Lücke barg die Möglichkeit, eine Datei von PCs zu stehlen, indem ein Datenpaket an User geschickt wurde, das Skype abstürzen ließ.
Dezember 2006	In mehreren Ländern verbreitete sich ein Wurm, der Workstations, auf denen Skype eingesetzt wurde, im Chatmodus infizierte.

Eine aktuelle Quelle die solche Angriffe dokumentiert bietet Skype selbst unter folgender Adresse: <http://www.skype.de/intl/de/security/>. Man sollte sich jedoch darüber klar sein, dass ein Hacker meistens gar kein großes Interesse hat, eine ausnützbar Lücke zu melden. Die Gefahr, dass diese Lücke jemand anderes findet, der sie publizieren könnte, wird durch die Tatsache, dass Skype closed code ist, auch nicht gefördert. Es ist also aufgrund der nicht offenliegenden Architektur schlecht abzuschätzen, wie viele Lücken noch existieren. Um Skype vor dem Zugriff von Drittprogrammen noch weiter abzuschotten, sollte bei der Skype Business Version die API-Schnittstelle, falls diese nicht dringend benötigt wird, z.B. für die Archivierung von Chatprotokollen, per Registrierungseintrag deaktiviert werden.

Viren, Würmer und Trojaner

Die gute Nachricht gibt es zuerst. Wenn man der auf IM Sicherheit spezialisierten Firma Akonix glauben darf, gab es seit 2006 bis jetzt weit über 1.300 verschiedene Angriffe durch Viren und Trojaner auf das IM Umfeld. Nur zwei davon zielten auf Skype ab und diese mussten sich auch noch der aktiven, teilweise fahrlässigen Mithilfe des Benutzers versichern, um ihr Unwesen zu treiben. Hierbei wird den potentiellen Opfern in der Regel über Chat oder Dateitransfer unvermittelt eine Schaddatei zum Download angeboten, die einmal vom Benutzer aufgerufen, den Kreislauf von neuen anstößt.

Eine zentrale Ausfilterung von potenziell schädlichen Dateien, wie es in Unternehmen oft beim Emailempfang praktiziert wird, ist aufgrund der verschlüsselten Übertragung nicht möglich. Mögliche Erkennungssignaturen von Schadprogrammen werden durch die

Verschlüsselung unkenntlich. Somit bleibt nur ein praktikabler Weg, der eigentlich bereits Standard sein sollte. Nach der Entschlüsselung der Daten steht die potenzielle Schadsoftware wieder mit erkennbarer Signatur im Speicher des Empfangsrechners. Hier kann eine Antivirensoftware eingreifen und das Schadprogramm vor der Ausführung abfangen. Dies wird auch von Skype empfohlen und liefert noch folgendes Diagramm, welches das Vorgehen veranschaulicht:

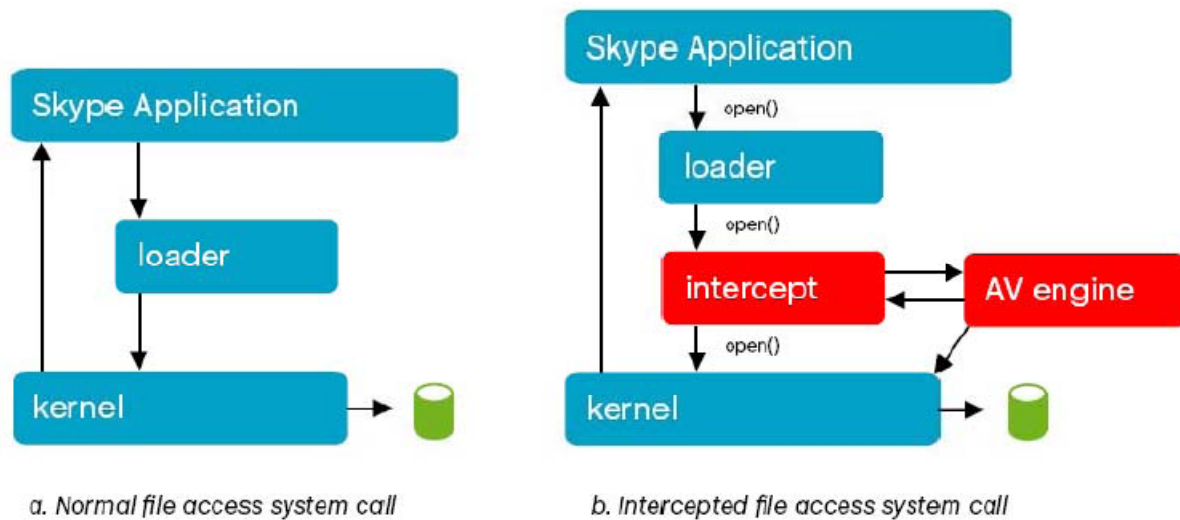


Abbildung 3: Antivirensoftware und Skype

Weiter einschränken lassen sich diese Angriffsszenarien nur in der Skype Business Version, in welcher sich per Registrierungseintrag die Dateitransferfunktionalität unterdrücken lässt oder durch ein Programm namens „SandboxIE“ welches Skype oder auch jedes andere verdächtige Programm in eine Quarantäneumgebung (sog. Sandbox) laufen lässt. Dabei werden alle Schreibprozesse auf die Festplatte durch die Sandbox verhindert, wodurch sich keine Schadsoftware „einnisten“ kann. Somit lässt sich keine transferierte Datei speichern, auch Chats werden nicht mehr dauerhaft protokolliert.

Belastung des Netzes

Ein oft schon mythisch ins Feld geführter Aspekt von Skype ist, dass der Client sich unter bestimmten Voraussetzungen zum super node entwickeln kann. Die Folge wäre, dass zur Abwicklung und Verwaltung von zumeist unternehmensfremder Kommunikation, kostbare Netzwerk- und Bandbreitenressourcen ohne entsprechenden Mehrwert für das eigene Unternehmen verbraucht werden würden. Auf den ersten Blick ist der Einwand sicher berechtigt, aber wie realistisch ist dieses Szenario wirklich? Skype selbst [1] und der Report von Michael Cough [4] geben Aufschluss darüber und legen u.a. drei Hauptkriterien fest:

1. **Die Laufzeit.** Um für das Skype-Netzwerk als verlässlicher super node in Betracht gezogen zu werden, muss der Rechner eine gewisse Zeit kontinuierlich am Netz sein, zumeist mehrere Tage. Dieses Kriterium erfüllen die meisten Bürorechner nicht, da diese je nach Arbeitstag zumindest einmal in 24 Stunden heruntergefahren werden.
2. **Keine Firewall.** Für einen super node wäre es sehr hinderlich hinter einer Firewall arbeiten zu müssen, da zu verwaltenden Verbindungen, die auf zufällig gewählten Ports eintreffen, geblockt werden würden. Somit ist dies ein weiteres Kriterium, das einen Skype-Client nicht mutieren lässt, da Unternehmensnetze zumeist durch Firewalls geschützt sind.

3. **Direkte Internetadresse.** Die IP-Adresse des Rechners muss dem direkten Internetadresspool angehören. Ist die Adresse des Rechners beispielsweise aus dem IP-Adressraum 192.168.xxx.xxx oder 10.xxx.xxx.xxx, handelt es sich um, für private Netze reservierte, Adressen. Auch in solch einer Umgebung mutiert Skype nicht.

Somit ist davon auszugehen, dass die Angst Skype könnte im Unternehmen zum super node mutieren eher theoretischer Natur ist, denn welcher von Mitarbeitern genutzte Firmenrechner läuft über mehrere Tage ohne Firewall mit direkter Internetadresse. Es sei noch ergänzend erwähnt, dass sich bei der Skype Business Version, die super node „Mutation“ per Registrierungseintrag unterdrücken lässt. Skype legt auch den Bandbreitenverbrauch der Software fest. Folgende Tabelle gibt einen Überblick:

Skype Client Ruhezustand:	0 – 0,5 KB pro Sekunde
Skype Client im Gebrauch:	5 – 16 KB pro Sekunde
Skype Supernode:	0 – 5 KB pro Sekunde; maximalbegrenzt
Skype Relay – Dateitransfer:	0 – 3 KB pro Sekunde und Sitzung; maximalbegrenzt
Skype Relay – Telefonat	0 – 4 KB pro Sekunde und Sitzung
Skype Relay – Videotelefonat:	0 – 10 KB pro Sekunde und Sitzung; maximalbegrenzt

Ein Relay als Vermittler hat die Möglichkeit mehrere Sitzungen zu bedienen, dies ist laut Skype aber eher ungewöhnlich.

Skype unter Kontrolle bringen oder loswerden, wenn es sein muss

Nun gibt es sicher Unternehmen bzw. Unternehmensbereiche in der Skype aufgrund der dargestellten Risiken absolut nicht tragbar ist. Als IT-Verantwortlicher steht man vor der Aufgabe ein Netzwerk von vielleicht einigen hundert Rechnern auf Skype-Installationen zu überprüfen, ggf. Installationen zu löschen und Re-Installationsversuche zu verhindern. Dies alles vor dem Hintergrund, dass Skype keine Administrationsrechte benötigt, um installiert zu werden. Ohne spezialisierte Werkzeuge ist diese Aufgabe nur mit fast unzumutbarem Aufwand zu lösen. Aber auch hier hat die Entwicklung nicht halt gemacht und einige Firmen haben sich dieser Herausforderung gestellt. Hier nun ein kleiner Überblick:

- L7 Skype Manager von Akonix (<http://www.akonix.com/>)
- Enterprise Threat Shield von SurfControl (<http://www.surfcontrol.com/>)
- Skypekiller von IS Decisions (<http://www.skypekiller.com/>)
- Skype_Check und Skype_Delete von Michael Gough (<http://www.skypetips.com/>)
- Und weitere...

Besonderes Augenmerk sollte auf Rechner gelegt werden, die nur kurzzeitig am Netz sind. Paradebeispiel sind Laptops von Außendienstmitarbeitern, die per VPN Zugang zum Unternehmensnetz haben. Hier kann eventuell ein Script, das beim Login ausgeführt wird, die gewünschten Behandlungsroutinen gegenüber eventuellen Skype-Installationen ausführen. Weitere Ansatzpunkte, die nicht den Anspruch auf 100%-ige Sicherheit haben, aber Skype das Leben erschweren, wären, den Zugang zu den wichtigsten Downloadadressen von Skype (Nr.1: www.skype.com,...) zu sperren, so dass jene Seiten von Mitarbeitern nicht geöffnet werden können. Oder falls Windows XP SP2 auf den Rechnern installiert ist, kann durch ein Kommandozeilenbefehl die windowseigene Firewall dazu veranlasst werden, Skype mit folgendem Befehl zu blocken:

“netsh firewall set allowedprogram C:\progra~1\Skype\phone\skype.exe Skype disable” [4]

Der Faktor Mensch

Der Benutzer liebt Skype, das Unternehmen manchmal auch

Nun der Benutzer, besonders im internationalen Umfeld und oft mit einer Perspektive jenseits jeglicher Unternehmensrisiken, liebt Skype. Einen typischen Eindruck Skype's beschreibt Katharina Lütke in einem Report [7] der u.a. den Untertitel „Skype aus der Sicht einer Userin“ beinhaltet. Beginnend mit der einfachen Installation bis zur Bedienung, Skype ist eingängig, simpel und intuitiv zu bedienen und läuft in den meisten Firmenumgebungen. Sie müssen Auslandsgespräche mühselig genehmigen lassen? Sie haben Emailbeschränkungen? Sie arbeiten gemeinsam an einem Projekt und müssen darum oft Konferenzen beschwerlich und zeitaufwendig anberaumen. Vergessen Sie es! Nehmen Sie Skype und machen Sie sich das Leben einfach. Auch Unternehmen können dadurch einen produktiven Vorteil haben, dass sofort und unkompliziert Sachverhalte geklärt werden können und das günstig, schnell und in besserer Sprachqualität als mit dem Telefon. Der Nutzer bevorzugt funktionierende Werkzeuge dieser Art und möchte sie bald nicht mehr missen, da sie schnell Teil seiner Kommunikationskultur werden.

Umgang mit unternehmenskritischen Daten

Trotzdem sollte auch die Kombination Mensch und Skype mit einer gesunden Portion Argwohn betrachtet werden. Wie bereits angesprochen, kann Gefahr für das Unternehmen durch das Laden von Schadprogrammen aus dem Internet bestehen. Aber auch in gegenläufiger Richtung, durch einen möglichen Informationsabfluss vom Unternehmen nach außen, besteht Gefahr. Die Studie von InfoWatch und dem russischen Online-Portal SecurityLab.ru hat auch diese Befürchtungen ausgewertet.

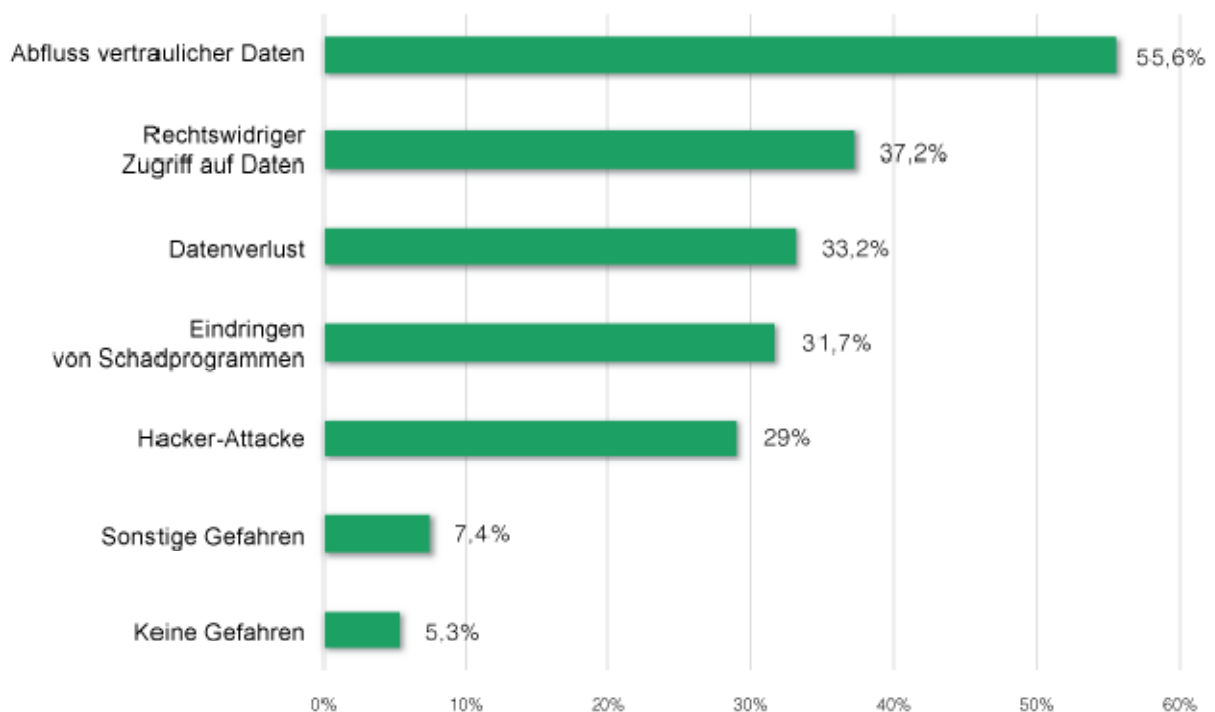


Abbildung 4: Umfrageergebnis zum Thema „Risiken bei der Anwendung von Skype“

Das Ergebnis ist nicht verwunderlich, schließlich leben die Unternehmen von Vorsprung an Know-How gegenüber Ihrer Konkurrenz. Wer kann effektiv ausschließen, dass einem eigenen fähigen Mitarbeiter in Schlüsselposition und finanzieller Notlage ein unverschämtes gutes

Bargeldangebot der Konkurrenz gemacht wird, um deren Forschungsbudget niedrig zu halten. Ein Klick auf Dateitransfer genügt und wichtige Daten können internetweit versendet werden. Andererseits sollten die Mitarbeiter nicht unter Generalverdacht gestellt und etwas auf die Loyalität vertraut werden.

Social Hacking

Bisher wurde davon ausgegangen, dass möglicherweise bewusst durch Mitarbeiter Daten geschmuggelt werden könnten. Viel häufiger und deshalb eine größere Bedrohung kann „Social Hacking“ sein. Aus dem Email-Umfeld ist das ja bekannt. Wer bekommt nicht mindestens 3 ominöse Emails pro Woche in denen man aufgefordert wird, seine Kontodaten samt PIN und mindestens fünf TANs auf einer gefälschten Bankseite einzugeben (Phishing). Hier wird also versucht den Mitarbeiter infolge von unbewusster Leichtsinnigkeit zur Ausführung einer bestimmten Aktion zu verleiten. Auf diese Weise konnten sich, wie beschrieben, alle Skypewürmer der letzten eineinhalb Jahre verbreiten. Grundsätzlich sind zwei große Angriffsszenarien denkbar:

1. Es wird per Dateitransfer ein Schadprogramm zum Download und Ausführung angeboten.
2. Per Chat wird ein Link übertragen, auf dessen Zielseite sich ein Schadprogramm befindet.

Wie bereits vorgetragen ist dieses Szenario der Bedrohung durch verseuchte Email sehr ähnlich. Für IT-Spezialisten im Unternehmensumfeld ist dies tatsächlich das größte Risiko, wie die Studie von InfoWatch und dem russischen Online-Portal SecurityLab.ru [8] weiter zeigt.

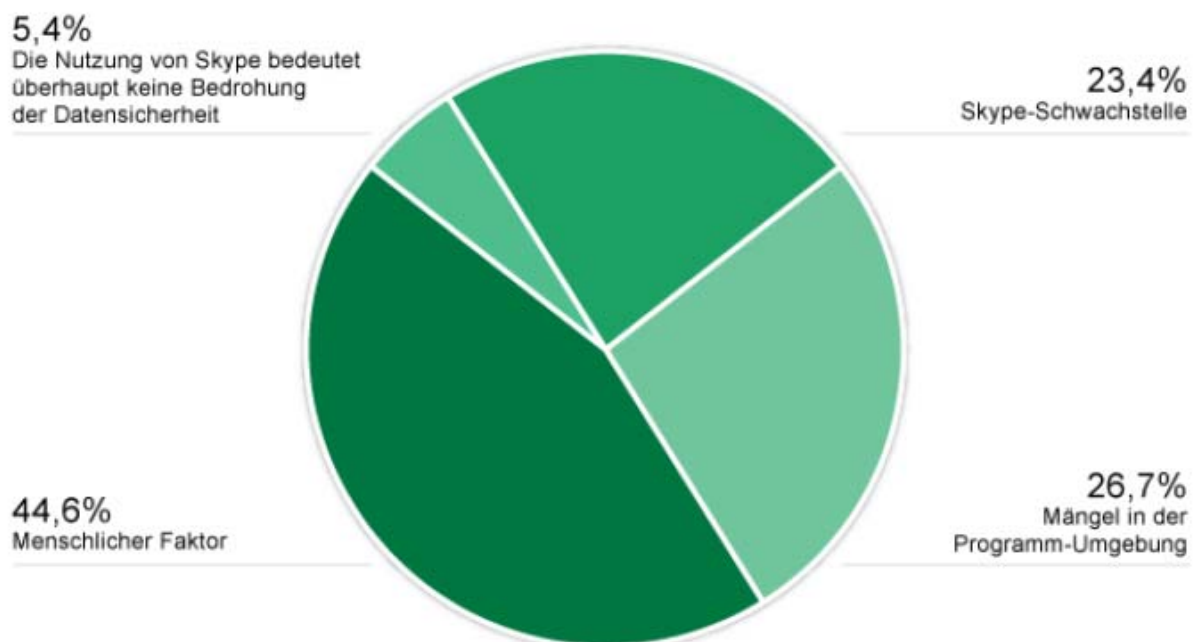


Abbildung 5: Umfrageergebnis zum Thema „Natur der Risiken bei der Verwendung von Skype“

Hier hilft nur konsequente Aufklärung und Sensibilisierung der Mitarbeiter gegenüber entsprechender Gefahren. Auch wieder der Hinweis auf Skype Business und das Abschalten der Dateitransferfunktionalität.

Skype auf dem USB-Stick

Das ist sozusagen der „Supergau“ für IT-Sicherheitsverantwortliche, denn hier kreuzen sich zwei Risikogruppen. In vielen Unternehmen sind auch USB-Sticks ins Auge der Betrachtung gerückt. Daumennagelgroße Gigabyte-Sticks sind keine Seltenheit mehr. Der mögliche Zufluss von Schadprogrammen und Abfluss von unternehmenskritischer Information durch USB-Sticks insbesondere durch die Verwendung von Autostart-Einträgen, ist ein separat zu betrachtendes Gebiet, weshalb nicht weiter darauf eingegangen wird. Wichtig zu wissen ist, dass es auf diese Weise möglich ist, Skype zu benutzen, auch wenn die Installation an sich durch Abwehrmaßnahmen nicht möglich wäre. Skype ist hier nämlich lauffertig auf dem USB-Stick installiert, und hinterlässt keine Spuren, da alle temporären Dateien, die zur Benutzung nötig sind, auf dem USB-Stick als Laufwerk abgelegt werden. Wird der Stick abgezogen und die Anwendung geschlossen, ist nicht nachzuweisen, dass Skype jemals auf dem Rechner war.

Abhilfe kann geschafft werden, wenn man den USB-Laufwerkstreiber von Windows per Sicherheitsrichtlinie und/oder Registrierungseintrag so einstellt, dass die Benutzung von USB-Laufwerken nicht mehr möglich ist. Für Netzwerkadministratoren gibt es ein Tool namens „USB Remote Drive Disabler“ der Firma IntelliNavigator Inc., der dies bequem über das Netzwerk bewerkstelligen kann.

Empfehlung und Fazit

Ganz grundlegend sollte erst einmal die Entscheidung getroffen werden, ob Skype im Unternehmen zugelassen wird oder nicht. Falls nicht, muss das System gegen unerlaubte Installation geschützt werden und entsprechende Sicherheitsrichtlinien und Arbeitsvertragszusätze aufgesetzt werden, die über das Verbot informieren.

Falls es erlaubt wird, sollte einzig und allein auch die Business-Version von Skype eingesetzt werden dürfen, da diese der betreffenden Firma die meiste Kontrolle einräumt. Wie und wo der Zugang zum Skype-Netzwerk erlaubt wird, muss dann in einem separaten Projekt geplant werden. Essentiell ist es allerdings, dass das betroffene Personal im Umgang mit Skype geschult und über sie konkreten Gefahren aufgeklärt wird, denn wie zu sehen war, braucht Schadsoftware in der Regel die aktive Mithilfe der Benutzer, um ihre Wirkung zu entfalten. Ebenfalls muss festgesetzt werden, dass nur von der Firma legitimierte Skype-Versionen benutzt werden dürfen und keine private Skype-Software „eingeschleppt“ wird. Dies sollte ebenfalls in einer Sicherheitsrichtlinie fixiert werden.

Literaturverzeichnis

- [1] **Skype Guide.** Skype Limited.
Guide for Network Administrators.
[Online] 31. Oktober 2006. [Zitat vom: 22. April 2007.]
<http://www.skype.com/security/guide-for-network-admins-30beta.pdf>
- [2] **Ruess, Nicolai.** Universität Ulm.
Skype.
[Online] November 2006. [Zitat vom: 22. April 2007.]
<http://www-vs.informatik.uni-ulm.de/teach/ws06/p2p/talks/papers/ruess.pdf>
- [3] **Schänzer, S.** BDG GmbH & Co KG.
Skype - Eine Gefahr für die Informationssicherheit in Unternehmen.
[Online] 21. August 2006. [Zitat vom: 22. April 2007.]
https://www.bdg.de/start/downloads/bdg_whitepapers/BDG_Skype.pdf
- [4] **Gough, Michael.** Computerworld - Networking&Internet.
How to protect your network against Skype.
[Online] 6. März 2007. [Zitat vom: 22. April 2007.]
<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9012243>
- [5] **Berson, Tom.** Anagram Laboratories.
SKYPE SECURITY EVALUATION.
[Online] 18. Oktober 2005. [Zitat vom: 22. April 2007.]
<http://www.skype.com/security/files/2005-031%20security%20evaluation.pdf>
- [6] **silicon.de.** silicon.de - Technologie und Business.
Sicherheitsexperte sieht Skype unter Druck.
[Online] 08. August 2006. [Zitat vom: 22. April 2007.]
http://www.silicon.de/enid/security_management/21761
- [7] **Lüthke, Katharina.** Social Software mit dunkler Seite.
Skype aus der Sicht einer Userin.
[Online] Juni 2006. [Zitat vom: 17. April 2007.]
<http://comment.univie.ac.at/06-2/27/> N 1605-4733 .
- [8] **InfoWatch, SecurityLab.ru.**
Die Sicherheit von Skype im Unternehmensumfeld.
[Online] 27. März 2007. [Zitat vom: 17. April 2007.]
<http://www.infowatch.com/de/threats?chapter=162971949&id=16>