Instant Messaging

Eine Analyse bezüglich Datensicherheit & Datenschutz am Beispiel von ICQ und XMPP

Autor: Marcel Graef

Studiengang: Medieninformatik Bachelor (5. Semester)

Lehrveranstaltung: IT-Sicherheit

Betreuer: Prof. Dr. rer. nat. Uwe Petermann

Erstellungsdatum: 30.12.2010

Inhaltsverzeichnis

1 Einleitung

Egal ob über ein Web-Interface oder einen Instant Messaging (IM)-Client-Kurznachrichten lassen sich einfach versenden. Diese Arbeit untersucht den IT-Grundschutz bezüglich Instant Messaging nach der Modellierung des Bundesamt für Sicherheit in der Informationstechnik (BSI). Die Untersuchung erstreckt sich über die Schicht 1, welche die übergreifenden Aspekte darstellt und die Schicht 5, die Client-Anwendung von Instant Messaging nach dem Fünf-Schichtenmodell. Die Sicherheit der Infrastruktur (Schicht 2), der IT-Systeme (Schicht 3) und der Netze (Schicht 4) werden nicht untersucht, da es zum Einen in der Hand des Anbieters liegt und zum Anderen mannigfaltige Strukturen im Wide Area Network (WAN)/ Local Area Network (LAN) gibt. Zudem existieren schon viele Bausteine zu den Gefährdungen und Maßnahmen.

Nach einem kurzen Überblick in Kapitel 2, in dem das allgemeine Funktionsprinzip und die Bedrohungen bezüglich IT-Sicherheit dargelegt werden, folgt eine kurze Zusammenfassung über den BSI-Baustein „Instant Messaging“ in Kapitel 3. Danach werden die Protokolle I seek you (ICQ) und Extensible Messaging and Presence Protocol (XMPP) einzeln auf IM-spezifische Gefährdungen untersucht und Lösungsvorschläge aufgezeigt. Kapitel 5 zeigt einen Weg für eine sichere Kommunikation auf und dient als Orientierungshilfe. Abrundend werden die rechtlichen Aspekte der IM-Dienste erörtert und ein Resümee zwischen ICQ und XMPP wird vollzogen.

2 Instant Messaging - ein Überblick

Im grundsätzlichen Prinzip sind sich die IM-Protokolle ähnlich. Es gibt eine Datenbank mit den Nutzerdaten der Kommunikationsteilnehmer. Die Kommunikationen zwischen den Teilnehmern werden über Server gesteuert und aufgebaut (siehe Abbildung 1). Bezüglich der Funktionalitäten zwischen den verschieden Protokollen gibt es diverse Unterschiede. Ein grober Vergleich ist in Tabelle 1 zu finden. Dabei bedeutet „✓“, dass der Dienst unterstützt wird und „x“, dass keine Unterstützung vorliegt.

[RRIMS, S. 1-40]

2.1 IM-Protokollunabhängige Angriffe

Grundsätzlich existieren unabhängig von den verwendeten Protokollen zahlreiche Angriffe, die die Grundprinzipien der IT-Sicherheit bei der Benutzung von IM verletzen. Konkret

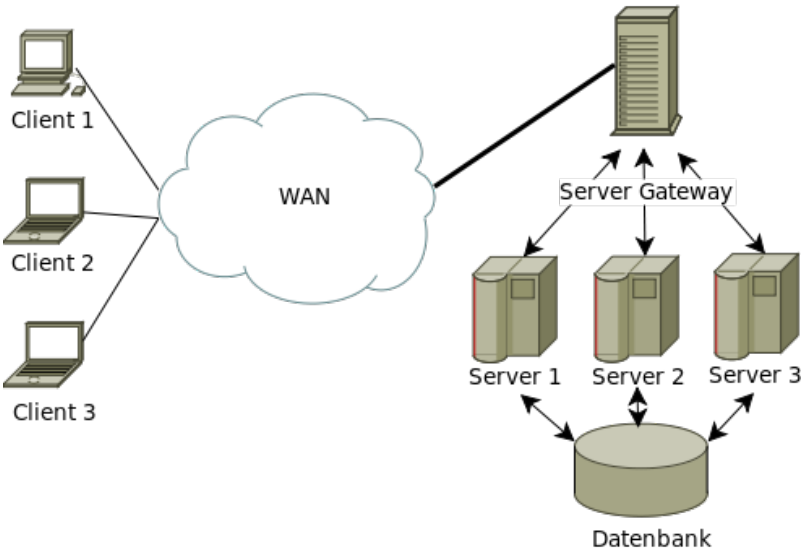

Abbildung 1: Funktionsprinzip Instant Messaging

IM Feature	AIM	MSN	YAHOO!	ICQ	XMPP
Instant Messaging	✓	✓	✓	✓	✓
Voice Chat	✓	✓	✓	✓	✓
Video Chat	x	✓	✓	✓	✓
Application Sharing	x	✓	x	x	x
File Transfer	✓	✓	✓	✓	✓
File Sharing	✓	x	✓	✓	x
Game Requests	✓	x	x	x	x
Remote Assistance	x	✓	x	x	x
Whiteboard	x	✓	x	x	x
IM Images	✓	x	x	x	✓

Tabelle 1: Vergleich der IM-Protokolle [RRIMS, S. 40]

sind dies Angriffe auf die Verfügbarkeit (Denial of Service), zum Beispiel durch Überlastung der Server/des Netzes oder die physikalische Zerstörung. Eine weitere Gefahrenquelle sind Angriffe auf die Vertraulichkeit, bei denen der Angreifer an Daten gelangt, die nicht für ihn bestimmt sind. Das kann geschehen durch Sniffen der Netzwerkverbindung oder durch Spoofing, falls sich der Angreifer nicht im gleichen Netzwerksegment befindet. Mit den beiden letztgenannten Methoden ist es möglich, Passwörter zu erspähen und weitere Angriffe vorzubereiten. Des Weiteren sind Angriffe auf die Integrität der Daten denkbar. Die Varianten können vom Einfügen sinnloser Informationen über gezielte Manipulation bis hin zum vollständigen Löschen der Nachricht reichen. Im Regelfall wird dabei die Man-In-The-Middle-Attack angewandt, d.h. der Angreifer gibt sich als Empfänger E_a aus und erhält die

Nachricht N vom Sender S. Im nächsten Schritt gibt sich der Angreifer als Sender S_a aus und leitet die Nachricht N_a an den Empfänger E, den S vorgesehen hat, weiter. Als weitere Möglichkeit, um an Informationen zu gelangen, können Angriffe auf das lokale System des Clients genutzt werden. Der Angreifer muss demnach eine andere Schwachstelle des lokalen System ausnutzen, um an Daten zu gelangen. Realisiert werden kann dies durch das Herausfinden des Passwortes für einen Zugang zum Rechner durch Keylogger, Erraten oder durch Schwachstellen im Betriebssystem etc. [SchiIM, S. 19-23]

2.2 Datensicherheit/Privatsphäre

Eine der zentralen Forderungen für ein gutes Nachrichtensystem ist, dass es hinreichend einfach sein muss mit anderen in Kontakt zu treten, aber auch schwer genug, um eine Belästigung durch unerwünschten Nachrichten zu vermeiden. Aus diesem Grund bieten viele IM-Systeme die Möglichkeit, erst nach einer gegenseitigen Bestätigung mit einander in Kontakt zu treten und meist werden dann erst die Statusinformationen für den anderen sichtbar. Zu beachten ist, dass aus diesen Informationen Persönlichkeitsprofile erstellt werden können, da der Benutzer einfach anhand eines/r Benutzernamens /-nummer unabhängig von der IP-Adresse identifiziert werden kann. Es ist möglich Informationen abzuleiten, z.B. wann der Benutzer in der Arbeit, zu Hause ist. Es ist demnach notwendig besonders darauf zu achten, wer diese Statusinformationen sehen darf und wie der Nutzer dies steuern kann. Des Weiteren muss auch ein Blockieren der Nachrichten möglich sein, da fälschlicherweise eine Zustellerlaubnis erteilt worden sein kann. [SchiIM, S. 24-26]

2.3 Datenschutz

Bei der Frage nach dem Datenschutz gilt es zunächst allgemeine Aspekte zu betrachten, die eng mit den persönlichen Interessen verbunden sind. Jeder Nutzer muss sich die Frage beantworten, welche Informationen er im schlimmsten Fall allen anderen Menschen zur Verfügung stellen möchte und welche Folgen dies für ihn hat. Dabei muss unbedingt beachtet werden, dass die Abschätzung der Folgen sehr eng damit verbunden ist, was zur Zeit technisch möglich ist und dass die Daten, sofern sie einmal verfasst wurden, später ausgewertet werden können. Aus diesen Gründen ist das oberste Gebot der Datensparsamkeit einzuhalten. So ist abzuraten Geburtsdatum, Freizeitinteressen, Geschlecht und Adressen anzugeben und damit ein Kandidat für eine Werbekampagne zu werden. Interessanter ist für Angreifer jedoch die IP-Adresse, mit der gezielte Angriffe auf dem Rechner durchgeführt werden können oder mit

der sich der Ort des Benutzers bestimmen lässt. [SchiIM, S. 24-26]

Ein Nachrichtenverlauf in einem IM-Client kann viele Vorteile aufweisen. Zum Einen als Gedankenstütze und zum Anderen zur Nachweisbarkeit bei dem Einsatz von IM-Technologien im Unternehmen. Damit wird jedoch auch ein neuer Angriffspunkt geschaffen, da so der Angreifer komprimiert an Informationen gelangt. Es muss demnach eine Zugriffskontrolle auf die Log-Datei vorhanden sein, damit die Einträge nicht von unauthorisierten Benutzern gelesen und verändert werden können. [RRIMS, S. 85-94]

2.4 Sonstige Sicherheitsprobleme

In Unternehmen können Benutzer die IT-Sicherheit gefährden, wenn sie IM-Programme installieren. Falls dann ein Benutzer eine direkte Verbindung mit einem anderen über das IM-Protokoll eingeht, kann ein Angeifer bösartigen Programmcode einschleusen und ausführen. Mit einem IM-Programm wird jedoch auch ein recht unkontrollierbarer Kanal in das WAN geschaffen, durch den urheberrechtlich geschütztes Material und/oder sensible Unternehmensdaten in unbefugte Hände gelangen können. Die Installation von IM-Programmen kann mit Hilfe einer geordneten Benutzerrechteverwaltung eingeschränkt werden. Eine Kommunikation über ein IM-Netz lässt sich technisch nur mit enormem Aufwand verhindern. Das Sperren der Transmission Control Protocol (TCP)-Ports kann beispielweise durch die Benutzung webbasierter Systeme umgangen werden. Eine strenge Sicherheitsleitlinie, bei der die Nutzung von IM-Systemen verboten ist, ist oft die einzige wirtschaftliche Lösung. [SchiIM, S. 26-29]

3 BSI Baustein „Instant Messaging“

3.1 Gefährdungen

Eine Übersicht der Gefährdungen ist in der Tabelle 4 im Anhang A.1 aus dem BSI IT-Grundschutz Baustein „Instant Messaging“ dargestellt. Im Folgenden werden nur die für IM spezifischen Gefährdungen betrachtet. Als organinisatorische Gefährdung ist die mangelhafte Archivierung von Nachrichten zu betrachten, die besonders für Unternehmen bezüglich des Rechtsnachweises wichtig ist. Eine menschliche Fehlhandlung stellt die Benutzung externer Dienste (ICQ) dar, die etwaige Verstöße gegen Rechtsvorschriften darstellen können (siehe 6.1). Ein Technisches Versagen ist die Verbreitung von Schadprogrammen über präparierte Webseiten (Drive-by-Downloads). Hierbei handelt es sich um Hyperlinks in den Textnach-

richten. Die Zieladresse des Links führt zu einem Schadprogramm. Falls es herunter geladen und zur Auführung gebracht wird, kann es seine Schadwirkung entfalten. Eine andere Gefährdung ist die Programmierbarkeit von Tools und Anwendungen, über die eine Schnittstelle zu IM-Systemen geschaffen werden kann und ggf. ein Zugriff auf IM-Systeme gewährt wird. Letzteres kann zur unbefugten Offenlegung von Daten führen. Auch eine fehlende oder mangelhafte Protokollierung stellt eine Gefährdung dar, da das Audit so nicht quallitativ durchzuführen ist und u.U. Angriffe nicht entdeckt werden können. Vorsätzliche Handlungen wie Cyberbullying (psychologische Angriffe mit dem Ziel, Personen oder Organisationen zu diskreditieren) werden in dieser Arbeit nicht betrachtet. [MMBauS, S. 65-69], [MKITGS]

3.2 Maßnahmen

Zur wirksamen Risikominimierung muss eine Konzentration auf die Gefährdungen vorgenommen werden, die das höchste Schadenspotenzial aufweisen. Die erste Maßnahme ist die Konzeption der sicheren Nutzung von IM. Dabei ist ein Konzept zu erstellen, das eine Entscheidung trifft, ob öffentliche IM-Dienste genutzt werden dürfen, von wem oder ob ein eigenes IM-Netz aufgebaut werden soll. Danach ist der Einsatz von IM Systemen zu klären, d.h. welche Informationen über dieses IM-Netz ausgetauscht werden sollen. Daraus ist abzuleiten, ob ein Einsatz von Verschlüsselungsverfahren für IM notwendig ist und/oder eine Kontrolle der Integrität genügt. Nach diesen Betrachtungen ist eine Auswahl eines IM Dienstanbieters vorzunehmen, der den vorherigen Anforderungen genügt.

Im Betrieb von IM ist eine Prüfung der Identifikation von Kontakten vorzunehmen, bevor ein Kontakt in die Kontaktliste eines Mitarbeiters aufgenommen wird. Falls ein eigener IM-Server betrieben wird, ist er gegen Angriffe (z.B. Denial of Service) zu schützen, das Logging zu aktivieren und ein Filtersystem zum Blockieren von Spam einzurichten. Falls ein externer IM-Anbieter genutzt wird, so ist eine regelmäßige Kontrolle von Nutzungsbedingungen und AGBs durchzuführen. Auf dem lokalen Computer der Firma ist eine sichere Konfiguration der IM Clients durchzuführen. Es ist sicherzustellen, dass keine Passwörter gespeichert werden und die übertragenen Dateien auf Viren geprüft werden. Des Weiteren ist eine gelegentliche Kontrolle gespeicherter Empfänger- und Konfigurationsdaten vorzunehmen. So kann aus dem gespeicherten Verlauf eventuell eine Manipulation entdeckt werden oder der Administrator kann anhand der Konfigurationsdaten eine Veränderung feststellen.

Es ist auch ein Notfallplan festzulegen bei einem Verdacht auf Hijacking (gewaltsame Übernahme der Kommunikation), der den Angriff sofort unterbindet. Die vollständige Liste

der Maßnahmen aus dem BSI IT-Grundschutz Baustein „Instant Messaging“ ist in Tabelle 5 im Anhang A.2 dargestellt. [MKITGS], [MMBauS, S. 86-91]

4 Aufbau der Protokolle und Ableitung der Datensicherheit und des Datenschutzes

4.1 ICQ (OSCAR-Protokoll)

4.1.1 Funktionsweise des OSCAR-Protokolls

ICQ stellt das erste IM-Programm dar und wurde im November 1996 von einer kleinen israelischen start-up Firma namens Mirabilis veröffentlicht. 1998 wurden Mirabilis und ICQ von AOL übernommen. ICQ erlaubt das Versenden von Textnachrichten, Mehrbenutzer-Chats, Dateiaustausch etc.

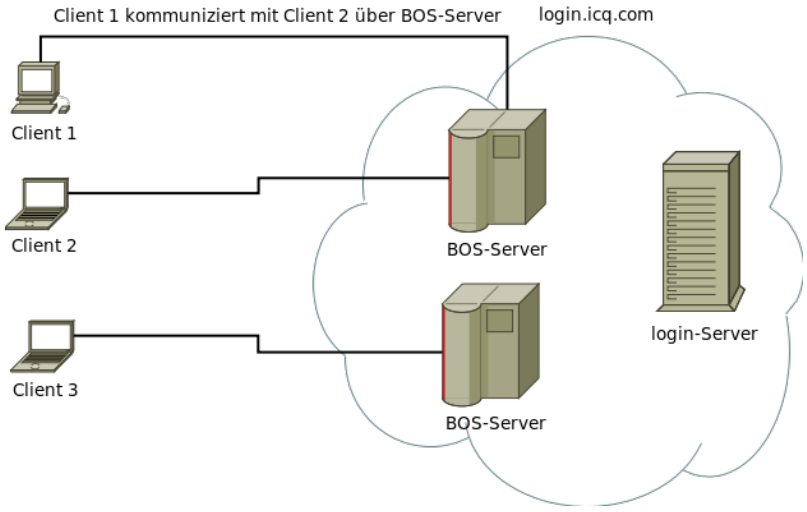

Abbildung 2: Informationsaustausch zwischen Clients über ICQ [SchiIM, S. 44]

Die Benutzer werden durch eine eindeutige Nummer Unique Identification Number (UIN) identifiziert. Seit der Übernahme von AOL gibt es das Protokoll Open System for Communication in Realtime (OSCAR), das sowohl ICQ als auch AOL Instant Messenger (AIM) beherrscht. Das OSCAR Protokoll ist ein auf einen binären Kommando basierendes Protokoll. Es wurde auch noch das Talk to OSCAR (TOC) (ASCII-basiert) als offenes Protokoll herausgegeben in der Hoffnung, dass Entwicker dieses statt des proprietären OSCAR verwenden. Im Folgenden wird das OSCAR-Protokoll für ICQ betrachtet, da es einige Unterschiede zwischen ICQ und AIM gibt. Informationen über das Protokoll wurden zum Großteil durch reverse engineering gewonnen. Der Login-Server ist login.icq.com und

verwendet Port 5190. Bei der Anmeldung am Server wird das Passwort mit der UIN übertragen. Seit dem 28. Mai 2008 wird das Passwort als MD5 Prüfsumme übertragen. Zuvor war es lediglich mit einem festen Schlüssel XOR-kodiert worden. Damit kann das Passwort nur noch mit höherem Aufwand ermittelt werden. Jedoch hat eine Protokollanalyse [SchiIM, S. 103] von OSCAR gezeigt, dass bei einer Änderung des Passwortes von einem Client aus dieses oft ungeschützt übertragen wird. Damit besteht die Möglichkeit des Abhörens eines Passwortes! Nach dem sich die Clientinstanz 1 bei dem Login-Server angemeldet hat, muss sie sich an dem Basic Oscar Service (BOS)-Server anmelden, um das IM-System zu nutzen.

Die Nachrichtenübertragung ist schematisch in Abbildung 2 dargestellt. In diesem Beispiel kommuniziert Client 1 mit Client 2 über den BOS-Server. Die Nachricht selbst wird unverschlüsselt im HTML-Format übertragen. Damit ist Abhören von Nutzdaten durch sniffen der Verbindung möglich. Die Verbindung zwischen Client und und BOS-Server bleibt während der gesamten Nutzung von ICQ bestehen. [RRIMS, S. 151-159], [SchiIM, S. 42-48], [WikICQ]

4.1.2 Bedrohungen der Schutzziele

Standardmäßig ist der Datentransfer ausgeschaltet. Wird er aktiviert, dann schickt S_A eine Anfrage an E_B. Falls E_B die Datei akzeptiert, kann Teilnehmer S_A eine Datei an E_B senden. Ist Teilnehmer S_A in der Buddy-Liste von E_B, so kann S_A auch ohne das S_B akzeptieren muss eine Datei senden. Dabei wird von Teilnehmer S_A über das Port 7320 eine direkte Verbindung zu E_B aufgebaut. Das ICQ-Protokoll ist für die schwache Authentifizierung, die fehlende Verschlüsselung und Einfachheit bekannt. In der Vergangenheit hat es zahlreiche erfolgreiche Denial of Service und remote buffer overflow Attacken gegeben. Des Weiteren konnten sich durch den einfachen Dateiaustausch rapide Trojanische Pferde und Würmer verbreiten. Zur Erhöhung des Datenschutzes ist notwendig, die Dateiübertragung zu verschlüsseln, da meist ein unsicherer Kommunikationsweg (WAN) benutzt wird. Aber es sind bei ICQ auch die rechtlichen Aspekte und Benutzungsbestimmungen zu beachten. Detaillierte Informationen sind in Kapitel 2.2 beschrieben. Um einen gezielten Angriff auf ein Opfer durchzuführen, ist die IP-Adresse des Opfers oft unumgänglich. Das ICQ-Protokoll bietet dafür beste Möglichkeiten. Die Dateiübertragung offenbart die IP-Adresse des Clients, wenn dieser Client eine Dateiübertragung, Sprachübertragung oder den automatischen Dateiaustausch aktiviert hat. Nun muss der Angreifer nur noch eine Schwachstelle im IT-System fin-

den und er kann weitere Angriffe, wie Denial-of-Service, Diebstahl der Identität/Passwörter durchführen.

Ein weiteres Feature das ICQ bietet ist das sogenannte „Message Logging“, also ein Mitschnitt der Nachrichten. Dies ist ein sehr komfortables Feature, aber es bringt auch große Datenschutzprobleme. Falls ein Angreifer in Besitz dieser Datei kommt, erhält er eine Unmenge an Informationen. Aus diesem Grund ist ein gesonderter Schutz der Log-Datei zu überdenken, etwa durch Verschlüsselung oder Verzicht auf einen Mitschnitt.

Eine weitere bestehende Bedrohung ist das Vortäuschen einer fremden Identität. Um dies zu erreichen, muss es dem Angreifer gelingen, eine neue Verbindung zum BOS-Server nach dem Empfang des Authorization Cookie und des Abbaus der Verbindung zum Authentifizierungsserver zu verhindern. Der Angreifer kann sich nun mit dem abgefangenen Authorization Cookie und der gefälschten IP-Adresse (IP-Spoofing) am BOS-Server anmelden.

Kurz zusammengefasst kann festgehalten werden, dass ICQ die Sicherheit eines Systems/Netzwerkes unnötig gefährdet. Zur Erhöhung der Sicherheit ist es absolut ratsam, die Weiterleitung der Pakete im Router, der sich zwischen LAN und WAN befindet für die drei obersten in der Tabelle 2 aufgeführten Ports zu deaktivieren.

Port	**Protokoll**	**Dienst**
3574	tcp	ICQ File Transfers
7320	tcp	ICQ File Sharing Images
6701	udp	ICQ Voice and Video chat services
4000	udp	ICQ
5190	tcp	login.icq.com (OSCAR)
9898	tcp	toc.oscar.aol.com (TOC)
3570	tcp	ICQ Messages

Tabelle 2: Portbelegung im ICQ-Protokoll [RRIMS, S. 151-159], [McAicq]

[RRIMS, S. 151-159], [SchiIM, S. 42-48], [WikICQ]

4.1.3 Schutzmaßnahmen

Es gibt nicht viel Möglichkeiten, die Nachrichtenkommunikation über OSCAR sicher zu gestalten. Falls kein Nutzungsrecht von ICQ Inc. verletzt werden soll, dürfen die Nachrichten nicht verschlüsselt werden. Einige OpenSource-Clients bieten die Ende-zu-Ende-Verschlüsselung mit Open Pretty Good Privacy (OpenPGP) und Off-the-Record Messaging (OTR) an. Dies funktioniert nur, wenn beide Kommunikationspartner die gleiche

Clientsoftware verwenden und es liegt streng genommen ein Verstoß gegen die Endbenutzungsbedingungen von ICQ Inc. vor (siehe 6.1). [SchiIM, S. 46], [TerICQ]

4.2 XMPP (Jabber)

4.2.1 Funktionsweise

Nach der RFC 3920 ist das XMPP ein Protokoll für das Streaming von Extensible Markup Language (XML)-Elementen in „Echtzeit“ zwischen verschiedenen Netzwerkknoten. Dabei handelt es sich um einen Informationsaustausch, der strukturiert ist. Beispielsweise können es Chatnachrichten oder Verfügbarkeitsinformationen sein. Zwischen Quelle und Senke besteht keine direkte Verbindung sondern die XMPP-Server vermitteln. Der Kommunikationspfad kann über mehrere Server verlaufen, wie in Abbildung 3 auf Seite 11 zu sehen ist.

Im Gegensatz zu ICQ ist die Adressierung bei XMPP ähnlich zu der beim e-mail-Verkehr. Eine sogenannte Jabber Identifier (JID) besteht aus einem Domainnamen (z.B. jabber.ccc.de), einem Knotennamen (user@jabber.ccc.de) und einer Angabe über die Ressourcen zur Nutzung verschiedener Clients (z.B. user@jabber.ccc.de/notebook). Damit muss jeder Anbieter/ Domainbetreiber nur auf die Eindeutigkeit seiner Knotennamen achten. Die Verbindung läuft wie folgt ab:

1. Der Client meldet sich beim Server (z.B. jabber.ccc.de) an.
2. Die XML-Nachricht (siehe Listing 1) wird an den Server geschickt.
3. Anhand der Ziel-JID wird die Nachricht an den Zielserver gesendet.
   (a) falls Benutzer mit JID angemeldet ist: Weiterleitung zum Benutzer
   (b) falls Benutzer offline: Zwischenspeicherung auf dem Server

Dabei ist zu beachten, dass der Server immer den Status des Clients kennt. Damit ist kein pollen von Seiten des Clients notwendig. Eine Nachricht kann drei Typen annehmen. Eine „message“ ist eine Nachricht zwischen zwei XMPP Benutzern. Die „presence“ dient zur Übermittlung von Informationen über den Status des Clients und „iq“ stellen Abfragen an den Server dar.

```
1 <message from="userA@jabber.ccc.de" to="userB@jabber.ccc.de">
2     <body>Ist dies eine OTR Verbindung?</body>
```

```
</message>
```

Listing 1: Aufbau XMPP-Nachricht

Das presence-Tag dient dazu den Status (verfügbar, abwesend, offline,...) eines Clients zu erfragen sowie den eigenen Status an den Server zu senden. Im Listing 2 ist eine Nachricht mit der Mitteilung „verfügbar“ zu sehen. Damit weiß der Server zu jeder Zeit, welchen Status der Client hat. Ein pollen von Seiten des Servers ist nicht notwendig.

```
<presence xml:lang="en">
    <show>dnd</show>
    <status>Wooing Juliet</status>
    <status xml:lang="cz">Ja dvo&#x0159;&#x00ED;m Juliet</status>
</presence>
```

Listing 2: Aufbau XMPP-Informationen

Das iq-Tag ist eine Information/Query und dient für Request/Response-Anfragen (z.B. für Rosteranfragen). Im Listing 3 ist eine Abfrage vom Client der Kontaktliste (Roster) zum Server zu sehen.

```
<iq from="juliet@example.com/balcony" type="get" id="roster_1">
    <query xmlns="jabber:iq:roster"/>
</iq>
```

Listing 3: Aufbau XMPP-der Kontaktliste Server

[StroJa], [XMPRFC], [KolbJa]

Pro Stream wird ein XML-Dokument angelegt und ist erst nach Beendigung des Streams vollständig. Die einzelnen XML-Elemente sind die Informationsträger, die Bedeutung dieser wird anhand der Elementbezeichner durch einen XML-Namensraum eindeutig definiert. [KolbJa]

Der XMPP-Server übernimmt neben der Anmeldung des Clients und der Steuerung auch die Kommunikation mit weiteren Serverinstanzen. Damit eine Server-Server-Verbindung im dezentralen XMPP-Netz über TCP möglich ist, werden im Domain Name System (DNS) in den (Service) Resource Records (SVR) die Server mit Dienst eingetragen. Der Informationsaustausch erfolgt auch hier über XML-Anweisungen. Mit ihnen ist die gesamte Steuerung der Server möglich. Um auch die Kommunikation mit anderen Protokollen (ICQ, Internet Relay Chat (IRC), AIM, etc.) zu kommunizieren, kann eine

Gateway-Komponente (XMPP-Transport) im XMPP-Server benutzt werden. Dies ist nicht zu verwechseln mit der Funktionsweise von Multi-Protokoll-Clients. Beim XMPP-Transport übersetzt sozusagen der Server zwischen den Protokollen. Will ein XMPP-Nutzer einem ICQ-Nutzer eine Nachricht senden, so muss er dem XMPP-Transport UIN und Passwort mitteilen. Der XMPP-Transprot loggt sich dann im ICQ-Netz ein und führt die Kommunikation. In Abbildung 3 ist Kommunikation schematisch dargestellt.

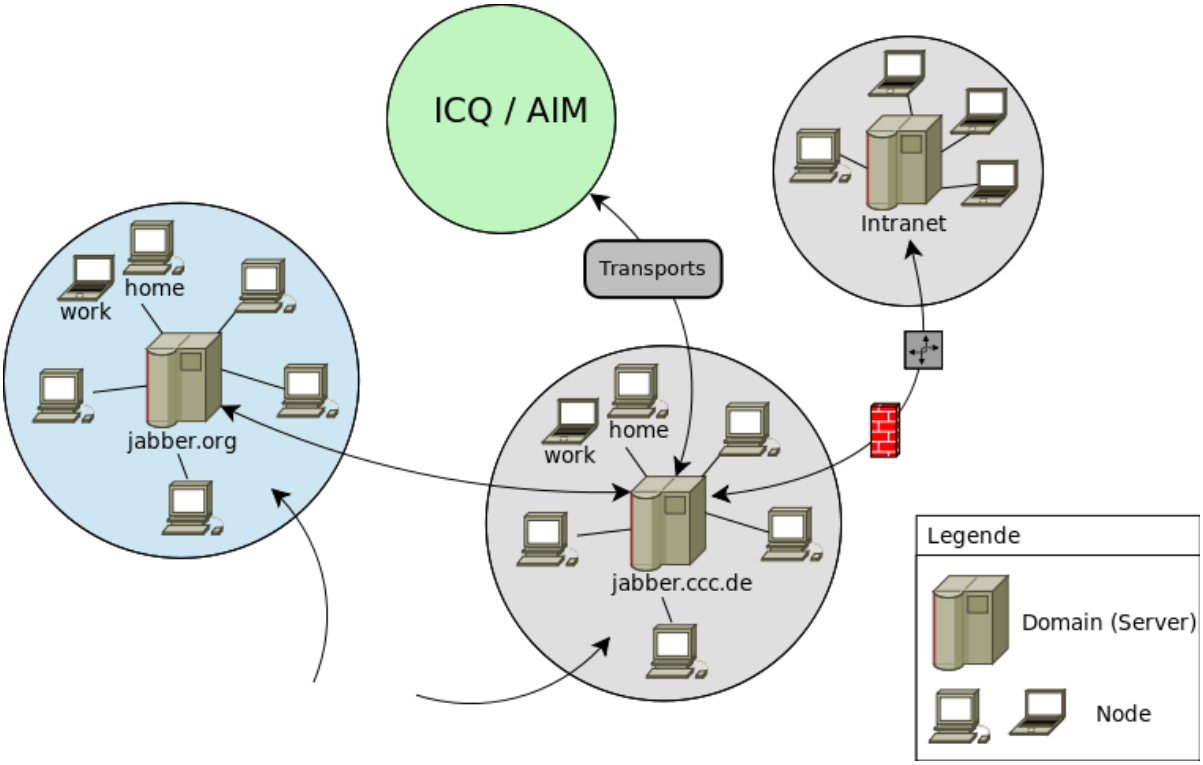

Abbildung 3: Kommunikation im XMPP-Netz

[SchiIM], [RRIMS, S. 54-66]

4.2.2 Funktionalitäten

Es werden eine ganze Reihe von Funktionen unterstützt und stetig werden diese erweitert. 2005 wurde XMPP um P2P-Fähigkeiten erweitert sowie die Spezifikation einer ersten Anwendung, „Jingle Audio“ für VoIP implementiert. Konferenzen mit mehreren Personen werden ebenso unterstützt wie die Übertragung von Dateien.

Des Weiteren bietet XMPP die Möglichkeit, die Verbindung von Client zu Server mit Secure Sockets Layer (SSL)/Transport Layer Security (TLS) zu verschlüsseln. Bei diesem Verfahren muss dies keinen Mehrgewinn in Bezug auf die Sicherheit darstellen. Wenn z.B. die Kommunikation zwischen den Servern unverschlüsselt ist, kann problemlos mitgehört werden. Dies würde eine **Verletzung der Vertraulichkeit** darstellen. Aus die-

sem Grund ist eine Server-zu-Server-Verschlüsselung dringend zu empfehlen. Aber dennoch stellen die Server auch mit der Kombination von Server-zu-Server- und Client-zu-Server-Verschlüsselung einen Angriffspunkt dar, da hier die Nachricht entschlüsselt vorliegt.

Abhilfe schafft die Client-zu-Client-Verschlüsselung. Viele Anbieter geben ihr den Vorzug, da weniger Ressourcen benötigt werden. Für den Datenschutz hat diese Variante den Vorteil, dass der Dienstanbieter nicht mithören kann. Dafür gibt es verschiedene Methoden. U.a. definiert die RFC 3923 Methoden zu der End-to-End-Signierung und Verschlüsselung. Weitere Verfahren sind OpenPGP (asymmetrisch) und OTR. [WikiJa], [SchiIM]

4.2.3 Anwendungen

Da hinter XMPP keine Organisation steckt und es ein frei zugängliches Protokoll darstellt, bietet XMPP wesentlich mehr Anwendungsgebiete als andere IM-Protokolle, wie z.B. ICQ. Das Auswärtige Amt nutzt über einen sicheren Kanal XMPP. Firmen können ebenfalls einen eigenen XMPP-Server installieren und so sicher intern kommunizieren.

Ein sehr wichtiger Punkt für die Integration eines IM-Dienstes in eigenen Anwendungen ist vor allem die Unterstützung von XMPP in den Skript- und Programmiersprachen. Auch in diesem Punkt führt XMPP. Es gibt Bibliotheken u.a. für Java (smack, JSO), php (Xmpphp.PHP), C (iksemel), Perl (Net::Jaber) und Python (Xmpppy). Des Weiteren bietet XMPP eine Interoperabilität mit anderen Protokollen und ist beliebig erweiterbar. [SchiIM]

4.2.4 Bedrohungen durch XMPP

Es existieren vom Protokoll XMPP her die üblichen Verletzlichkeiten gegenüber Integrität und Vertraulichkeit, wenn keiner der oben genannten Verschlüsselungsalgorithmen verwendet wird. Dies ist ganz klar: Da die Nachricht und das Passwort hierbei in XML im Klartext übertragen wird, kann sie/es gelesen werden durch sniffen der Verbindung und die Nachricht kann manipuliert werden.

Um XMPP die Vertraulichkeit und Integrität zu gewährleisten, muss eine Kombination von Client-Server-Verschlüsselung (damit das Passwort verschlüsselt in XML übertragen wird) und Ende-zu-Ende-Verschlüsselung (damit die Nachricht nicht gelesen werden kann) eingesetzt werden. Am besten ist hier eine Kombination aus Ende-zu-Ende-, Client-Server- und Server-Server-Verschlüsselung. Bei den verwendeten Verschlüsselungsverfahren ist darauf zu achten, dass die Sicherheit nicht durch Geheimhaltung der Verfahren gegeben ist, sondern durch das Verfahren an sich (no security by obscurity). Dies ist bei OpenPGP,

OTR und dem spezifizierten Verfahren in der RFC 3923 der Fall.

Für das offene Protokoll XMPP gibt es eine Vielzahl an Client-Programmen, die durch die Sicherheit, die XMPP in Kombination mit den Verschlüsselungsalgorithmen bietet, oft angegriffen werden. So wurden bei dem Programm Pidgin 2.5.6 2009 zwei Buffer Overflows gefunden, - zum Einem in der Verarbeitung von Microsoft Network (MSN)-Service Location Protocol (SLP)-Nachrichten und zum Anderen im XMPP-SOCKS5-Server bei dem Aufbau von ausgehenden Verbindungen für den Dateitransfer. [BacPid], [RRIMS, S. 85, 132, 214]

5 Sicherer kommunizieren – Ein Anfang. Go Jabber!

XMPP hat sich noch nicht stark etabliert, obwohl die technische Überlegenheit offensichtlich ist. Im Gegensatz zu ICQ/MSN/AIM/Yahoo! Ist es dezentral organisiert und vermeidet damit die Schaffung eines zentralen Servers, der ein potentielles Ausfallrisiko und einen Angriffspunkt darstellt. Bei XMPP besteht die Möglichkeit zum Aufbau einer SSL-Verbindung, die mit 128Bit oder höher verschlüsselt ist genauso wie die Verwendung von XMPP über das Tor-Netzwerk.

Tor dient zum Anonymisieren von Anwendungen in Kombination mit Privacy Enhancing Proxy (Privoxy), was die Privatsphäre stärkt wird ein leistungsfähiges Paket zum anonymen Datenaustausch geschaffen. Um letzteres bequem nutzen zu können, wird auf dem lokalen Computer ein Privoxy zusammen mit Tor eingerichtet. Im IM-Client wird dann der entsprechende Proxy (SOCKS5) eingetragen, sofern dies der Client unterstützt. Diese Variante ist nicht nur auf XMPP beschränkt, sondern gilt auch für ICQ/AIM/etc.

Neben der Anonymität ist die Geheimhaltung für den Datenschutz und die Datensicherheit ein bedeutendes Schutzziel. Hier setzt OTR an und stellt eine Ende-zu-Ende-Verschlüsselung bereit. OTR stellt dabei eine Kombination des symmetrischen Kryptoverfahrens Advanced Encryption Standard (AES), des Diffie-Hellman-Schlüsselaustauschs und der Hashfunktion SHA-1 dar. Mit OTR ist eine Verschlüsselung, Abstreitbarkeit und Zurechenbarkeit der Nachricht möglich. Vorteilhaft ist bei OTR, dass bei der Übertragung nicht festgestellt werden kann, ob ein bestimmter Schlüssel von einer bestimmten Person verwendet wurde. Bei der Authentifizierung eines Kommunikationspartners ist darauf zu achten, dass die gemeinsame Passphrase auf einem anderen Kanal (z.B. per Post) ausgetauscht wird. Auch von einem automatischen Fingerprint-Abgleich ist abzuraten. Für viele Client-Programme (u.a. Pidgin) gibt es Plugins. Falls dies nicht der Fall ist kann ein

Proxy mit OTR eingerichtet werden. Ein zentrales Problem bei OTR ist, dass beide Kommunikationspartner OTR installiert haben müssen.

Das XMPP-Protokoll und OTR-Verfahren sind im Gegensatz zu ICQ,AIM, MSN und Yahoo! offene Standards. Dadurch wird die Sicherheit nicht durch Geheimhaltung gewährleistet sondern durch das Verfahren selbst. [MarCCC], [HolzJa], [OTRWik], [OTRCyp]

6 Rechtliche Aspekte

6.1 ICQ stellt eine Bedrohung für den Datenschutz dar

Der folgende Auszug aus den AGBs (Notice of Acknowledgment) von ICQ Inc. verdeutlicht die mögliche Beeinträchtigung des informellen Selbstbestimmungsrechtes.:

> *[...] You agree that by posting any material or information anywhere on the ICQ Services and Information you surrender your copyright and any other proprietary right in the posted material or information. You further agree that ICQ LLC. is entitled to use at its own discretion any of the posted material or information in any manner it deems fit, including, but not limited to, publishing the material or distributing it. [...] [AckICQ]*

Damit besteht die Möglichkeit, dass auf den Servern von ICQ Inc. Dienste laufen könnten, welche die gesandten Nachrichten auswerten. Die rechtliche Grundlage für solche AGBs ist in Deutschland nicht vorhanden. Aber ICQ Inc. hat zur Zeit keinen einzigen Server in Deutschland, weshalb das amerikanische Recht gilt. Mit der Zustimmung zu den AGBs drückt man eindeutig aus, dass man nichts gegen eine Weitergabe der vesandten Informationen einzuwenden hat.[TerICQ]

Ein mögliches Szenario: ICQ Inc. hat damit das Recht e-mail Adressen und Telefonnummern, welche über den Dienst versandt wurden, an Werbefirmen zu verkaufen. Es können aber auch Informationen an die Musikindustrie oder an den jeweiligen Staat geleitet werden.[TerICQ]

Diese rechtlichen Bestimmungen machen es unmöglich ICQ in einem Unternehmen einzusetzen, da Firmengeheimnisse so nicht mehr Eigentum der Firma sind. Durch die Nutzung von ICQ, wurden dessen Nutzungsbedingungen anerkannt und Verwertungsrechte an den übertragenen Informationen eingeräumt. Ein Aufbau eines eigenen Netzes mit OSCAR ist durch die Architektur (siehe Abschnitt 4.1) insbesondere der UIN von ICQ nicht möglich.

Wichtig ist auch, dass ICQ grundsätzlich die Benutzung alternativer Clientsoftware (z.B. Pidgin) verbietet, somit ist eine End-zu-Ende-Verschlüsselung gemäß Endbenutzer-Lizenzvertrag nicht gestattet. Der folgende Auszug aus den Nutzungsbeschränkungen (Restrictions on Use) von ICQ verdeutlicht dies.

> *You agree not to (1) create or use any software other than the Software provided by ICQ, or any affiliate thereof, to enter your ICQ number and password or to access the ICQ Services, without the express written authorization of ICQ; (2) extract information from the ICQ Services, reverse engineer, decompile, disassemble, alter, duplicate, make copies, create derivative works from, distribute or provide others with the Software, the ICQ communications protocol or any information available on, derived or extracted from the ICQ Services, or any part thereof; (3) block, disable or otherwise affect any advertising, advertisement banner window, links to other sites and services, or other features that constitute an integral part of the Software and ICQ Services; [...] [EULICQ]*

6.2 Ist bei XMPP alles besser?

Grundsätztlich gestattet XMPP eine werbefreie Kommunikation. XMPP erlaubt Vielfalt durch ein von Grund auf dezentrales System. Daraus lassen sich zwei Dinge ableiten. Es ist durch die Dezentralisierung ein kompletter Ausfall des Netzes unmöglich. Zudem kann sich ein Pluralismus bezüglich der Nutzungsbedingungen, Dienste und Features etablieren. Aus diesen Gründen kann die Frage, wie es mit dem Datenschutz bei XMPP gestellt ist nicht beantwortet werden. Es gibt unzählige XMPP-Server, der Nutzer hat hier die Wahl und falls kein passendes Angebot dabei ist besteht immer die Möglichkeit einen eigenen zu schaffen.

Zusammenfassend kann festgehalten werden, dass der XMPP-Server (jabber.ccc.de) alle sensiblen Daten nicht weitergibt an Dritte und nur für die Kommunikation notwendige Daten gespeichert werden. Das Clientprogramm Pidgin steht unter der GNU General Public License (GPL) und gibt damit keine Einschränkungen für Erweiterungen vor, wie etwa das OTR. OTR steht unter der GNU Lesser General Public License (LGPL) und ist damit für jeden frei zugänglich. [CCCXMP], [MKITGS]

7 Resümee

Die folgende Tabelle 3 stellt die wesentlichen Eigenschaften der zwei Dienste gegenüber.

Merkmale	**XMPP (Jabber)**	**ICQ (OSCAR)**
Lizenz	frei und offen	seit dem 05.03.2008 ist Spezifikation von OSCAR offen gelegt Standardversion ist closed Source
Verschlüsselung	SSL/TLS, OpenPGP, OTR	Verschüsselung zwischen Client-Server ist nicht möglich; Client-Client-Verschlüsselung funktioniert nur mit alternativer Clientsoftware
Werbung	keine Clients mit Werbung bekannt	der ICQ-Client von ICQ Inc. ist mit Werbung überfüllt, es gibt jedoch auch Clients die werbefrei sind aber nicht alle Funktionen anbieten
Mehrfachanmeldung	möglich, auch mit Priroritätsangabe	nicht möglich
Architektur	dezentral	zentral
Unternehmensgeeignet	ja	nein (siehe Abschnitt 6.1)
Benutzeraccount	JID ist an einen XMPP-Server gebunden	UIN wird zentral verwaltet
Passwort vergessen?	keine Möglichkeit das Passwort vom Server anzufordern	falls e-mail-Adresse beim Anmelden angegeben wird Passwort per Mail geschickt
Datenschutz	z.B jabber.ccc.de enthält keine kritischen Elemente	nicht gegeben (siehe Abschnitt 6.1)
Kommunikation mit anderen Protokollen	möglich über Transports	nur zu AIM

Tabelle 3: Vergleich XMPP & ICQ [BeckJa]

Literatur

[AckICQ] Moshe, Eliav: Notice of Acknowledgment. http://www.icq.com/legal/notice.html. aufgerufen am 21.12.2008.

[BacPid] Bachfeld, Daniel: Mehrere Sicherheitslücken in Pidgin 2.5.6 geschlossen. 22.05.2009. http://www.heise.de/security/meldung/Mehrere-Sicherheitsluecken-in-Pidgin-2-5-6-geschlossen-219851.html. aufgerufen am 27.12.2010.

[BeckJa] Becker, Felix: Instant Messaging to Instant Managing: Verteilte Informations- und Kommunikationssysteme zur Effizienzsteigerung / von Erik Mautsch http://blog.jbbr.net/against-icq. 27.12.2010.

[CCCXMP] Schwindt, Peter: Privacy - web.jabber.ccc.de. https://web.jabber.ccc.de/?page_id=5. aufgerufen am 27.12.2010.

[EULICQ] Moshe, Eliav: ICQ End User License Agreement. http://www.icq.com/legal/end-user-license.html. aufgerufen am 21.12.2008.

[HolzJa] Holzhauer, Florian: Eine kleine Einführung in Jabber - Chaos Seminar CCC Ulm. 14.03.2005. http://www.ulm.ccc.de/old/chaos-seminar/jabber/jabberpresentationccc.pdf. aufgerufen am 27.12.2010.

[KolbJa] Kolbe, Lukas: XMPP: Extensible Messaging and Presence Protocol. http://www.techfak.uni-bielefeld.de/∼swrede/xml-isy/talks/xmpp.pdf. aufgerufen am 18.12.2010.

[MarCCC] Warum Jabber statt ICQ/MSN/AIM/Y! http://www.ulm.ccc.de/ marcel/warum-jabber.htm. aufgerufen am 05.12.2010.

[McAicq] Corporate KnowledgeBase. https://kc.mcafee.com/corporate/index?page=content&id=KB69487&pmv=print. aufgerufen am 18.12.2010.

[MKITGS] Maybaum, Markus, Keller, Prof. Dr. Jörg: Wie sicher ist eigentlich Instant Messaging? Die Entstehung eines neuen IT-Grundschutz-Bausteins. in: BSI Forum, 6/2009. S. 49-52

[MMBauS] Maybaum, Markus (2009): Erstellung eines Bausteins „Instant Messaging“ für die IT-Grundschutz-Kataloge. https://www.bsi.bund.de/SharedDocs

/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Extern/Instant_Messaging_pdf.pdf?__blob=publicationFile. aufgerufen am 28.12.2010.

[OTRWik] Off-the-Record Messaging http://de.wikipedia.org/wiki/Off-the-Record_Messaging. aufgerufen am 21.12.2008.

[OTRCyp] Off-the-Record Messaging Protocol version 2 http://www.cypherpunks.ca/otr/Protocol-v2-3.1.0.html. aufgerufen am 21.12.2008.

[RRIMS] Rittinghouse, John W. und Ransome, James F. (2005): Instant Messaging Security. Burlington: Elsevier Digital Press.

[SchiIM] Schildt, Holger: Sicherheitsaspekte von Instant Messaging. http://www.bsz-bw.de/cgi-bin/xvms.cgi?SWB12103506., aufgerufen am 18.12.2010.

[StroJa] Strobel, Cornelia: Jabber- das Plaudern geht weiter: Vortrag zum Workshop Netz- und Service-Infrastrukturen, 19.-22.04.2004, Löbsal bei Meißen. http://www.bsz-bw.de/cgi-bin/xvms.cgi?SWB11163719. aufgerufen am 18.12.2010.

[TerICQ] Moshe, Eliav: ICQ Terms of Service. http://www.icq.com/legal. aufgerufen am 21.12.2008.

[WikICQ] ICQ. http://de.wikipedia.org/wiki/ICQ. aufgerufen am 18.12.2010.

[WikiJa] Extensible Messaging and Presence Protocol. http://de.wikipedia.org/wiki/Extensible_Messaging_and_Presence_Protocol. aufgerufen am 18.12.2010.

[XMPRFC] Saint-Andre, Peter: RFC 3921 (XMPP): Instant Messaging and Presence. http://tools.ietf.org/pdf/rfc3921.pdf. aufgerufen am 27.12.2010.

A Anhang

A.1 Gefährdungslage Instant Messaging

Nr.	Kurzbeschreibung	IM spez.
Organisatorische Mängel		
G 2.54	Vertraulichkeitsverlust durch Restinformation	
G 2.55	Ungeordnete Nutzung von Kommunikationssystemen	

Nr.	Kurzbeschreibung	IM spez.
G 2.56	Mangelhafte Beschreibung von Dateien	
G 2.87	Verwendung unsicherer Protokolle in unsicheren Netzen	
N 2.3	Mangelhafte Archivierung von Nachrichten	✓
Menschliche Fehlhandlungen		
G 3.13	Übertragung falscher oder nicht gewünschter Datensätze	
G 3.45	Unzureichende Identifikationsprüfung von Kommunikationspartnern	
N 3.2	Unbeabsichtigte Rechtsfolgen durch Nutzung externer Dienste	✓
Technisches Versagen		
G 4.32	Nichtzustellung einer Nachricht	
G 4.37	Mangelnde Authentizität und Vertraulichkeit von Nachrichten	
N 4.1	Verbreitung von Schadprogrammen über präparierte Webseiten (Drive-by-Downloads)	✓
N 4.2	Programmierbarkeit von Tools und Anwendungen	✓
N 4.3	Fehlende oder mangelhafte Protokollierung	✓
Vorsätzliche Handlungen		
G 5.72	Missbräuchliche Nutzung von Kommunikationssystemen	
G 5.73	Vortäuschen eines falschen Absenders	
G 5.75	Überlastung durch eingehende Nachrichten	
G 5.76	Mailbomben	
G 5.77	Mitlesen von Nachrichten	
G 5.89	Hijacking	
G 5.90	Manipulation von Adressbüchern und Verteilerlisten	
G 5.110	Web Bugs	
G 5.111	Missbrauch aktiver Inhalte in Nachrichten	
N 5.2	Cyberbullying	✓

Tabelle 4: Gefährdungen [MMBauS, S. 65-69]

A.2 Maßnahmenempfehlungen Instant Messaging

Erläuterungen der Abkürzungen:

A Einstiegsstufe

B Aufbaustufe

C Zertifikatstufe

Z zusätzliche Maßnahme

W Wissensmaßnahme

Nr.	Kurzbeschreibung	IM spez.
Planung und Konzeption		
M 2.122	(C) Einheitliche Adressen	
M 2.275	(Z) Einrichtung funktionsbezogener Adressen	
M 2.X.4	(A) Konzeption der sicheren Nutzung von Instant Messaging	✓
M 2.X.5	(A) Regelung für den Einsatz von Instant Messaging	✓
M 4.X.1	(A) Einsatz von Instant Messaging Systemen	✓
M 5.X.5	(A) Einsatz von Verschlüsselungsverfahren für Instant Messaging	✓
M 5.W.1	(W) Instant Messaging Protokolle Beschaffung	
Beschaffung		
M 2.X.1	(A) Auswahl eines Instant Messaging Dienstanbieters	✓
Umsetzung		
M 3.15	(B) Informationen für alle Mitarbeiter über die Nutzung von Kommunikationssystemen	
M 4.99	(C) Schutz gegen nachträgliche Veränderung von Informationen	
M 5.22	(A) Kompatibilitätsprüfung des Sender- und Empfängersystems	
M 5.32	(C) Sicherer Einsatz von Kommunikationssoftware	
M 5.47	(C) Einrichten einer Closed User Group	
Betrieb		
M 2.121	(B) Regelmäßiges Löschen von Nachrichten	
M 2.371	(C) Geregelte Deaktivierung und Löschung ungenutzter Konten	
M 2.X.2	(A) Prüfung der Identifikation von Kontakten	✓
M 2.X.7	(C) Regelmäßige Kontrolle von Nutzungsbedingungen und AGBs externer Dienste	✓

Nr.	Kurzbeschreibung	IM spez.
M 4.37	(A) Sperren bestimmter Absender	
M 4.64	(C) Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen	
M 4.199	(C) Vermeidung gefährlicher Datenformate	
M 5.53	(A) Schutz vor Mailbomben	
M 5.54	(B) Schutz vor Überlastung durch eingehende Nachrichten und Spam	
M 5.63	(C) Einsatz von GNU Privacy Guard (GnuPG) oder Pretty Good Privacy (PGP)	
M 5.69	(A) Schutz vor aktiven Inhalten	
M 5.108	(A) Kryptographische Absicherung von Nachrichten	
M 5.X.2	(A) Sicherer Betrieb eines Instant Messaging Servers	✓
M 5.X.3	(A) Sichere Konfiguration der Instant Messaging Clients	✓
M 5.X.4	(C) Gelegentliche Kontrolle gespeicherter Empfänger- und Konfigurationsdaten	✓
M 5.W.3	(W) Erkennen von Session Cookie Angriffen	
Notfallvorsorge		
M 6.X.1	(A) Verhalten bei Verdacht auf Hijacking	✓

Tabelle 5: Maßnahmen [MMBauS, S. 86-87]

Tabellenverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

AES Advanced Encryption Standard.

AIM AOL Instant Messenger.

BOS Basic Oscar Service.

BSI Bundesamt für Sicherheit in der Informationstechnik.

DNS Domain Name System.

GnuPG GNU Privacy Guard.

GPL GNU General Public License.

ICQ I seek you.

IM Instant Messaging.

IRC Internet Relay Chat.

JID Jabber Identifier.

LAN Local Area Network.

LGPL GNU Lesser General Public License.

MSN Microsoft Network.

OpenPGP Open Pretty Good Privacy.

OSCAR Open System for Communication in Realtime.

OTR Off-the-Record Messaging.

PGP Pretty Good Privacy.

Privoxy Privacy Enhancing Proxy.

SLP Service Location Protocol.

SSL Secure Sockets Layer.

SVR (Service) Resource Records.

TCP Transmission Control Protocol.

TLS Transport Layer Security.

TOC Talk to OSCAR.

UIN Unique Identification Number.

WAN Wide Area Network.

XML Extensible Markup Language.

XMPP Extensible Messaging and Presence Protocol.