

CASSARIUS

Unified Communications Security

Marcel Oberli

Head of Confidence

CASSARIUS AG

031 384 05 11

marcel.oberli@cassarius.ch



Geschäftseinheiten

CASSARIUS *Fortune*

Business und Informatik im Einklang.

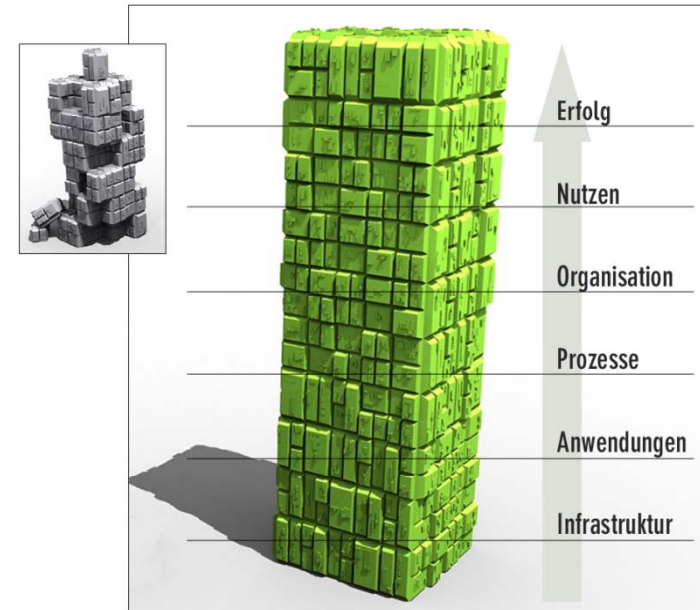
CASSARIUS *Solutions*

Individuelle Lösungen mit Garantie.

CASSARIUS *Confidence*

Vertrauen und Erfolg. Mit Sicherheit.

Wir beraten und unterstützen Sie in allen Fragen des sinnvollen Risiko- und Sicherheitsmanagement für die Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit Ihrer Informationen und Systeme.



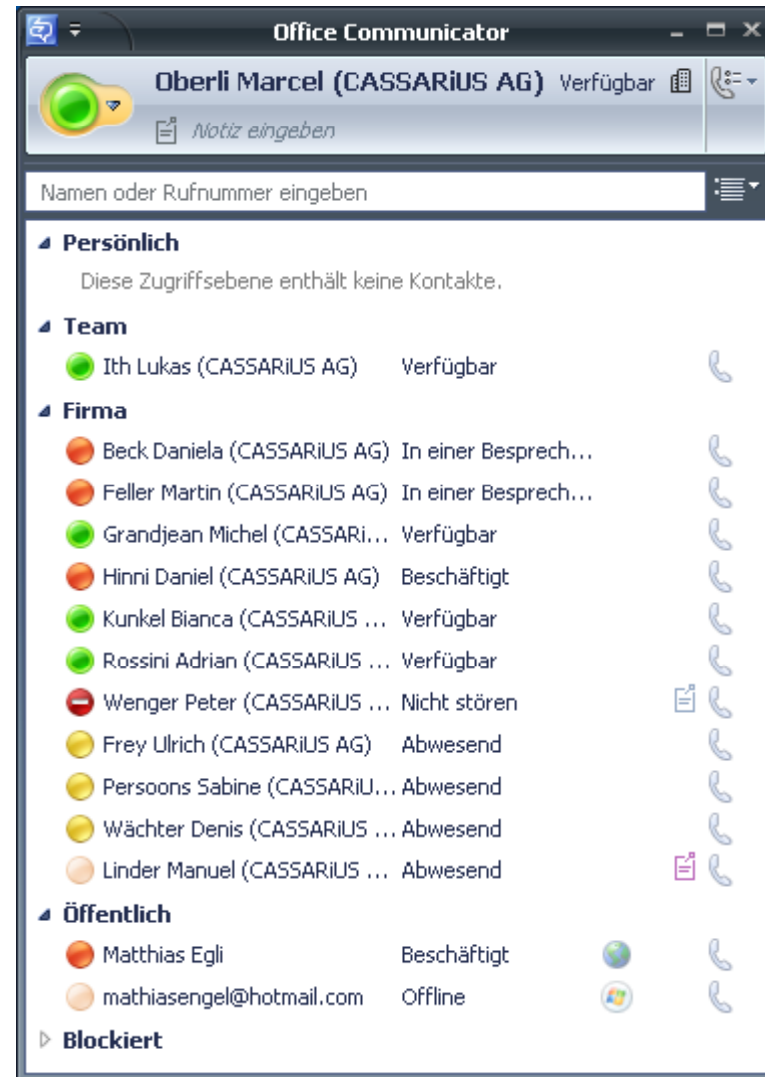


Agenda

- **(Sehr) kurze Einführung in Unified Communications am Beispiel von Microsoft**
- **Warum UC Security**
- **Federations**
- **Rechtliche Aspekte**

Was ist Unified Communications?

- Presence
- VoIP
- Instant Messaging
 - File Transfer
- Video Conferencing
- Voicemailbox in Outlook
- Shared Desktop





UC Security

Warum überhaupt?

Hemmschwellen gegen Unified Communications

Was spricht Ihrer Meinung nach gegen die Einführung einer UC-Lösung?
Mehrfachantworten möglich, in Prozent der befragten Unternehmen.

Kommunikationsbedürfnisse und -verhalten sind noch unklar	60%
Umstellungskosten	55%
Komplexität der Lösung selbst	42%
Komplexität der Umstellung/Integration	34%
Sicherheitsbedenken	30%
Mangelnde Akzeptanz der Benutzer	25%
Angebote sind noch nicht marktreif	24%
Mangelnde Transparenz auf dem Anbietermarkt	10%
Compliance-Gründe	10%
Mangelnde Unterstützung durch Mitarbeiter	10%

Quelle: MSM Research

Bedrohungen für Unified Communications

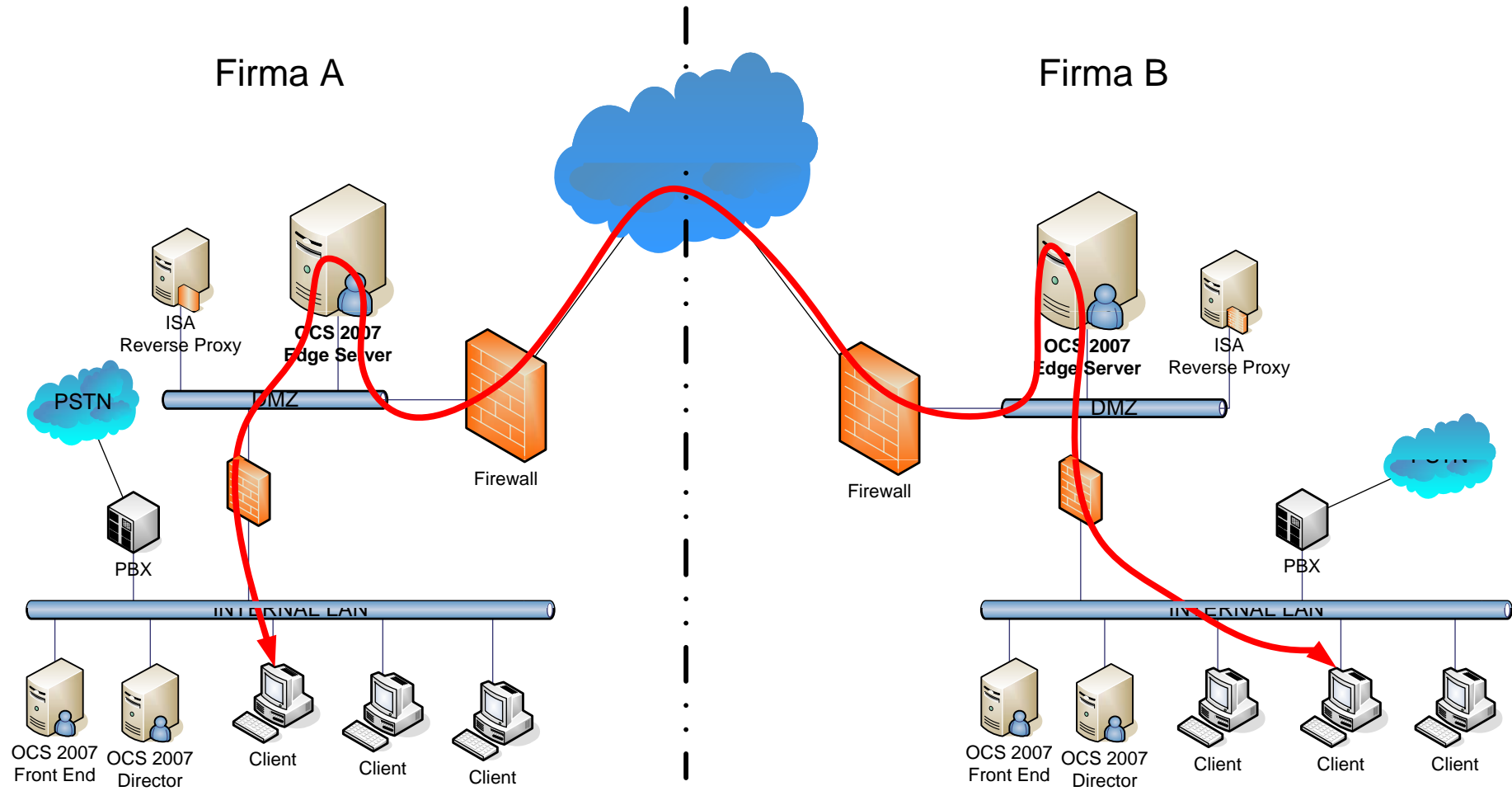
- **Vertraulichkeit**
 - Mithören, Mitlesen von Informationen (Voice, Text, Video)
 - Zugriff auf fremde Mailbox
 - Zugriff auf Informationen auf Server oder Client (Schwachstelle in Software)
 - Abhören von Gesprächen in fremdem Raum
 - Vortäuschen einer falschen Identität
- **Integrität (teilweise auch Nachvollziehbarkeit)**
 - Veränderung von Sprachdaten
 - Veränderung von Textmitteilungen
 - Manipulation der Signalisierung
 - Veränderung der Daten auf dem Server
- **Verfügbarkeit**
 - Denial of Service (Server, Client, Netzwerk)
 - Hardware / Software Probleme (Server, Netzwerk, Internet, Voice)
 - Verbreitung von Viren





Federations

Federations





Federations

- **Kommunikation zwischen verschiedenen Unternehmungen mit Microsoft UC**
- **Volle Kommunikation möglich**
 - **VoIP, Instant Messaging, Conferencing**
- **Können von Mitarbeitenden initiiert werden**
- **Kein manueller Eingriff der IT nötig**

Aufbau einer neuen Federation

1. Mitarbeiter fügt externen Kontakt hinzu
2. OCS Infrastruktur merkt, dass sich Kontakt ausserhalb der Unternehmung befindet
 - Weiterleitung der Anfrage an EDGE Server
3. EDGE Server merkt: es besteht keine Verbindung zu „schweizermeister.ch“
 - EDGE Server startet DNS SRV Abfrage (`_sipfederationtls._tcp.schweizermeister.ch`)
4. EDGE Server nimmt Verbindung zum EDGE Server von schweizermeister.ch auf
5. Federation wird hergestellt
6. Federation wird auf beiden Seiten gespeichert
7. Kommunikation kann via die EDGE Servers gestartet werden

Geben Sie die E-Mail- oder Anmeldeadresse der gesuchten Person ein.

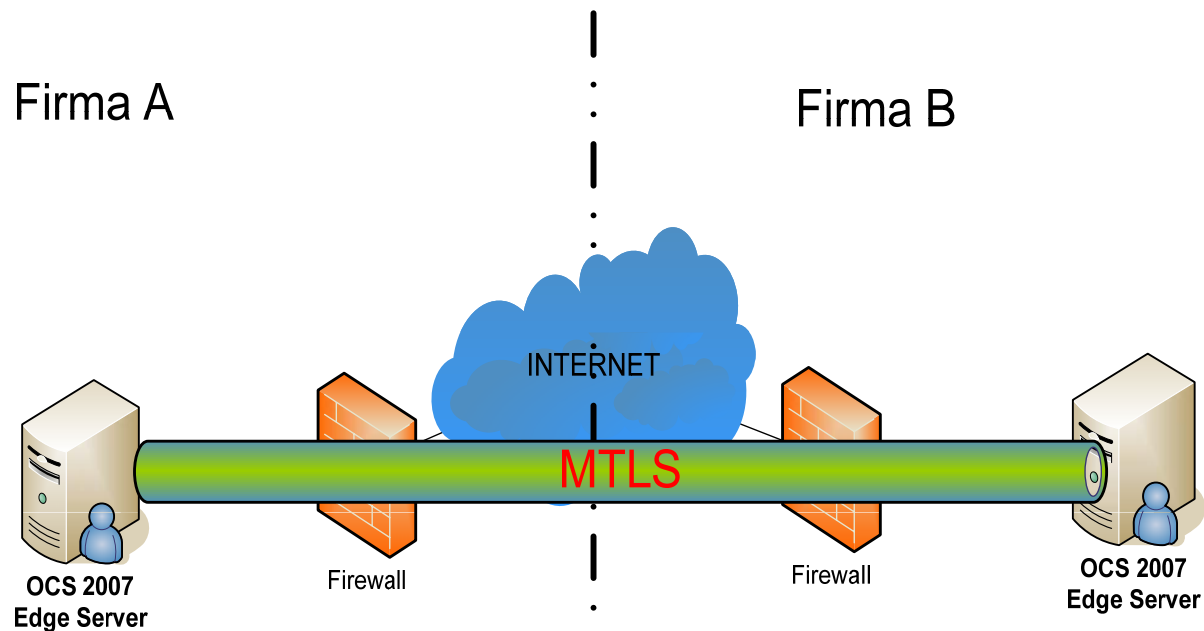


Federations: Bedrohungen

- **Vertraulichkeit**
 - Mithören von Nachrichten im Internet
- **Denial of service**
 - Lahmlegen des Edge Servers
- **Vortäuschen falscher Identität**
 - In Kontakt treten mit internen Mitarbeitenden
- **Brute Force Attacke auf E-Mail Adressen**
 - Durch gezieltes „hinzufügen“ von neuen Kontakten
- **Verbreitung von Viren / SPAM**

Federations: Massnahmen

- Vertraulichkeit
 - Verschlüsselung zwischen Edge Server
 - MTLS (gegenseitige Authentifikation)
 - Erfordert jeweils offizielle Zertifikate





Federations: Massnahmen

- **Vortäuschen falscher Identität**
 - **Offizielle Zertifikate auf Edge Servern**
 - Bekannte Domänen können nicht missbraucht werden
 - Unbekannte oder ähnliche Domänen schon: `seydou.doumbia@bsycb.ch`
 - **Gegenseitige Authentifikation der Server**
 - nicht aber der Mitarbeitenden
 - **Mitarbeiter Schulung**
 - Wie verhalte ich mich bei Federation Kontakten?
 - **Offizielle Zertifikate für jeden Benutzer**
 - Ist mit Microsoft OCS nicht möglich



Federations: Massnahmen

- **Brute Force Attacken auf E-Mail Adressen**
 - **Drosselung des Netzwerkverkehrs**
 - **Limitierte „message rate“**
 - **Dynamisch angepasst anhand einer Traffic Analyse**
 - **Viele falsche Anfragen = niedrige „message rate“**
 - **Limitierung der Kommunikation mit bestimmter Anzahl Usernames**
 - **Bestimmte Zeitspanne / Bestimmte Anzahl Usernames**
 - **Whitelist**



Federations: Massnahmen

- **Denial of Service Attacke**
 - Drosselung Bandbreite / Limitation Benutzernamen
 - Redundanzen
 - Kein effektiver Schutz



Federations: Massnahmen

- **Verbreitung Viren / SPAM**
 - **AntiVirus**
 - **Forefront Security for Office Communications Server**
 - **File Transfer deaktivieren**
 - **Schulung Mitarbeitende**



Rechtliche Aspekte



Wo ist das Problem?

- **Presence Information**
- **Überwachung (Big Brother)**
 - **Durch Arbeitgeber**
 - **Durch Kollegen**
- **Weigerung von Mitarbeitenden mit Unified Communications zu arbeiten**

Gesetzesartikel

- **Verhältnismässiges Bearbeiten von Personendaten, *DSG Art 4, Abs 2***
- **Schutz von Leben, Gesundheit und persönlicher Integrität der Arbeitnehmer, *OR Art. 328, Abs 2***
- **„Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen, dürfen nicht eingesetzt werden.“, *Verordnung 3 zum Arbeitsgesetz, Art. 26***





Lösung: Rechtliche Aspekte

- **WICHTIG:** Ziel und Zweck von Microsoft UC in einer Weisung klar definieren
- Sicherstellen, dass keine Überwachungen durch privilegierte Mitarbeitende durchgeführt werden

CASSARIUS

Unified Communications Security

Marcel Oberli

Head of Confidence

CASSARIUS AG

031 384 05 11

marcel.oberli@cassarius.ch

