Pierre Audoin Consultants

BERLECON RESEARCH
a PAC Company

White Paper

Wie sicher ist OpenScape Web Collaboration?

Ergebnisse einer Sicherheitsanalyse des Fraunhofer AISEC und Fraunhofer ESK

Fraunhofer AISEC

Fraunhofer ESK

Mai 2012

Inhaltsverzeichnis

3

1. ÜBERBLICK

Die Einführung von Web- und Videokonferenzlösungen ist aktuell ein Topthema, was jedoch mit zahlreichen Sicherheitsrisiken verbunden sein kann.

Die Einführung von Collaboration-Anwendungen, wie z. B. **Web- und Videokonferenzlösungen**, ist derzeit ein **Topthema** in vielen deutschen Unternehmen. Allerdings sollten sich Unternehmen darüber bewusst sein, dass die Nutzung von echtzeitbasierten Collaboration-Lösungen mit zahlreichen **Sicherheitsrisiken** verbunden sein kann**.** Denn wenn eine Vielzahl an Personen sich über unterschiedlichste Endgeräte und Netzzugänge in eine Konferenz einwählt oder ein (internetbasierter) Fernzugriff erfolgt, sind vermehrt Angriffspunkte gegeben, die die **Verfügbarkeit**, **Integrität**, **Vertraulichkeit** und **Authentizität** der ausgetauschen Informationen und Daten gefährden. Zahlreiche Gefahren wie Spoofing, Manipulationen, Sniffing oder Denial of Service-Attacken bedrohen dabei die Sicherheit **unternehmenssensibler Informationen** und **Daten**. Sicherheitsaspekte sollten daher bei der Auswahl einer Collaboration-Lösung eine zentrale Rolle spielen.

Zielgruppe: Unternehmen, die webbasierte Konferenz- und Fernwartungsanwendungen nutzen, aber damit einhergehende Risiken vermeiden möchten

Dieses White Paper zeigt auf, worauf Unternehmen beim Einsatz von webbasierten Konferenz- und Fernwartungsanwendungen achten sollten und wie die Lösung **OpenScape Web Collaboration** von **Siemens Enterprise Communications** verschiedene Sicherheitsrisiken adressiert und entsprechende Maßnahmen umsetzt.

OpenScape Web Collaboration: Theoretische und praktische Sicherheitsanalyse der Fraunhofer-Einrichtungen AISEC und ESK

Dazu wurde die Lösung von den **Fraunhofer-Einrichtungen** für Angewandte und Integrierte Sicherheit (**AISEC**) sowie für Systeme der Kommunikationstechnik (**ESK**) verschiedenen **theoretischen** und **praktischen Sicherheitsanalysen** unterzogen. Die Untersuchungen wurden von **August bis Dezember 2011** durchgeführt. Diese zeigen, dass mit den vorhandenen Sicherheitsmechanismen unter Berücksichtigung der hier gegebenen Empfehlungen eine **sichere Nutzung** von OpenScape Web Collaboration gewährleistet werden kann.

Methodik und Untersuchungsgegenstand

Technische Basis von OpenScape Web Collaboration ist FastViewer

OpenScape Web Collaboration basiert technisch auf dem **FastViewer**-Produkt, das von Siemens Enterprise Communications im Jahr 2010 übernommen und in das OpenScape-Portfolio integriert wurde. OpenScape Web Collaboration und FastViewer basieren damit auf der gleichen Software und verwenden die gleichen Sicherheitsmechanismen und Protokolle.

4

Abhängig vom Anwendungsbereich stehen bei OpenScape Web Collaboration verschiedene Produktversionen zur Verfügung.

OpenScape Web Collaboration wird als **eigenständige Collaboration-Lösung** sowie als **integrierbare Funktion** für OpenScape-Anwendungen angeboten. Darüber hinaus kann die Lösung sowohl **on-premise**, d. h. im Eigenbetrieb, als auch im **Cloud-Modell,** d. h. in der extern gehosteten Variante, bezogen werden.

Abhängig vom **Anwendungsbereich** werden bei OpenScape Web Collaboration **verschiedene Lizenzen** unterschieden, die sich in ihrem Funktionsumfang und der maximalen Teilnehmerzahl differenzieren:

- **OpenScape Secure Advisor** ist für den (internetbasierten) Zugriff auf entfernte Rechner ausgelegt, bspw. für den echtzeitbasierten IT-Support von Kunden und Endnutzern.
- Virtuelle Konferenzräume für eine Vielzahl an Nutzern, bspw. für Präsentationen und Online-Meetings, werden durch die Lösung **OpenScape Instant Meeting** abgebildet.

Im Rahmen der vorliegenden Sicherheitsuntersuchung wurden beide Produkte analysiert – sowohl in der On-premise-Variante[1] als auch in der cloud-basierten Variante. Abbildung 2 gibt einen schematischen Überblick über Untersuchungsgegenstand und Methodik der Sicherheitsanalyse.

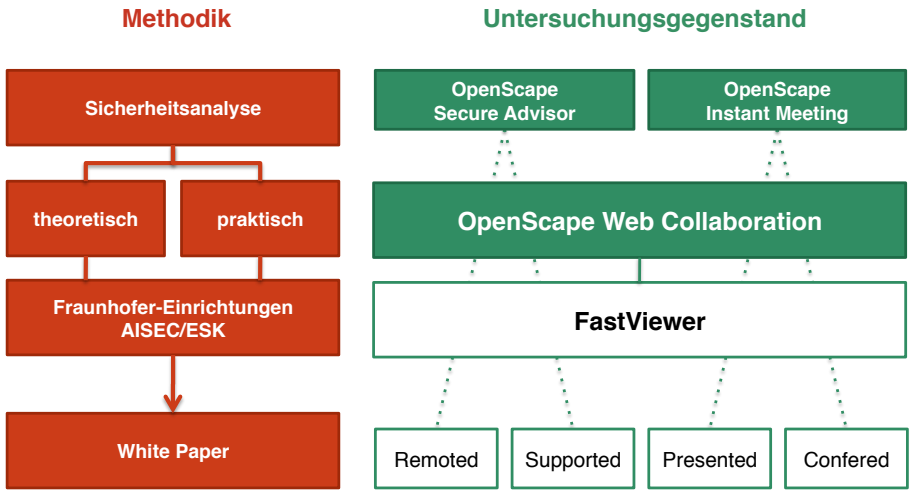

Abb. 1: Untersuchungsgegenstand und Methodik der Sicherheitsanalyse

[1] Hinweis: Bei der On-premise-Lösung verwenden Unternehmen zwar eine eigene Serverlösung (unabhängig von den Kommunikationsservern von Siemens Enterprise Communications), allerdings verwendet diese Variante die gleichen Sicherheitsstandards.

5

Sicherheitsanalyse untersuchte Authentizität, Integrität, Vertraulichkeit und Verfügbarkeit von OpenScape Web Collaboration

Die Analyseschwerpunkte lagen auf den typischen Sicherheitsaspekten Authentizität, Integrität, Vertraulichkeit und Verfügbarkeit der Lösung. Bei der **theoretischen Analyse** wurde die Umsetzung von Sicherheitsmechanismen anhand der Spezifikation analysiert. Sie setzte den Fokus vor allem auf die Sicherheit und Robustheit der Architektur sowie auf die Sicherheit der eingesetzten Übertragungstechniken und Protokolle. Zusätzlich wurde eine Bedrohungsanalyse umgesetzt, in der mögliche Angriffe identifiziert wurden. Bei der **praktischen Sicherheitsanalyse** wurde überprüft, ob und wie die sicherheitsrelevanten Spezifikationen (korrekt) umgesetzt wurden. Anhand eines Penetrations-Testes wurde schließlich systematisch nach Schwachstellen der Lösung gesucht.

6

2. SICHERHEITSASPEKTE VON COLLABORATION-LÖSUNGEN

2.1. Hintergrund

„Collaboration“ ist aktuell ein Topthema: 80 % der deutschen Unternehmen planen Investitionen.

Collaboration ist aktuell ein **Topthema** auf der Agenda vieler Unternehmen, wie eine aktuelle Studie von PAC/Berlecon zeigt: Mehr als **80 %** der deutschen Unternehmen planten im Jahr 2011 **Investitionen** in die Anschaffung und Integration von **Collaboration-Anwendungen**.[2] Dabei sollen vor allem webbasierte Lösungen zum „Document Sharing“ sowie für **Web- und Videokonferenzen** Mitarbeiter bei der effizienten Vernetzung und Zusammenarbeit unterstützen. So planen **40 %** der deutschen Unternehmen Investitionen in den Aus- und Aufbau von **Web- und Videokonferenzlösungen** (s. Abb. 1).

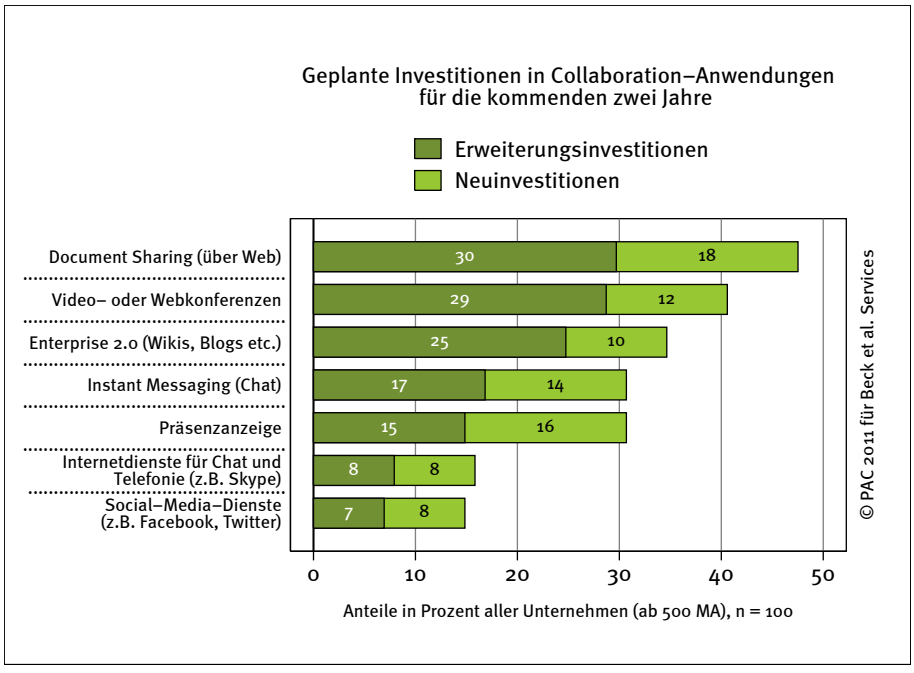

Abb. 2: Geplante Investitionen in Collaboration-Anwendungen

Allerdings sind mit der Nutzung von echtzeitbasierten Collaboration-Lösungen zahlreiche Sicherheitsrisiken verbunden.

Allerdings sollten sich Unternehmen darüber bewusst sein, dass die Nutzung von echtzeitbasierten Collaboration-Lösungen mit zahlreichen Sicherheitsrisiken verbunden sein kann, für die **herkömmliche Schutzmaßnahmen** häufig **nicht mehr ausreichen.** Denn wenn eine

[2] PAC/Berlecon (2011): IT Reality Check – Collaboration zwischen Anspruch und Wirklichkeit, ein Report im Auftrag von Beck et al. Services.

Vielzahl an Personen sich über unterschiedlichste Endgeräte und Netzzugänge bspw. in eine Konferenz einwählt oder ein internetbasierter Fernzugriff erfolgt, sind vermehrt Angriffspunkte gegeben, die die **Verfügbarkeit**, **Integrität**, **Vertraulichkeit** und **Authentizität** der ausgetauschen Informationen und Daten gefährden.

2.2. Sicherheitsrisiken und Schutzziele

Das Sicherheitskonzept sollte die Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität unternehmenssensibler Daten und Informationen berücksichtigen.

Sicherheitsaspekte sollten daher bei der Auswahl einer Collaboration-Lösung eine zentrale Rolle spielen. Das **Sicherheitskonzept** einer Webkonferenzlösung sollte insbesondere folgende **Schutzziele** berücksichtigen:[3]

- **Vertraulichkeit**: Collaboration-Lösungen müssen gewährleisten, dass nur autorisierte Nutzer bzw. Systeme einen Zugriff zur Lösung erlangen. Dies gilt insbesondere dann, wenn über Webkonferenzen strategische Unternehmensinformationen ausgetauscht werden, bspw. bei Management-Meetings oder Webkonferenzen von Research & Development-Teams. Adäquate Sicherheitsmechanismen müssen das unerlaubte Mithören oder Mitschneiden einer Konferenz oder den unberechtigten Zugriff auf abgelegte Dokumente, Teilnehmerdaten oder gesamte Rechner ausschließen. Um Informationen angemessen zu schützen, müssen u. a. Nutzungsberechtigungen vergeben und entzogen werden können und Daten immer verschlüsselt übertragen werden.
- **Verfügbarkeit**: Die Funktionsfähigkeit und Stabilität einer Collaboration-Lösung ist zentral. Insbesondere wenn eine Vielzahl an Personen involviert ist und eine echtzeitbasierte Videoübertragung stattfindet, werden hohe Ansprüche an die Verfügbarkeit der Serversysteme (Bandbreite) gestellt. Werden bspw. vertriebsorientierte Webcasts mit potentiellen Kunden abgehalten, ist das reibungslose Funktionieren der Konferenzlösung ein geschäftskritischer Erfolgsfaktor. Insbesondere bei cloud-basierten Systemen, die den Risiken öffentlicher Netze ausgesetzt sind, bedarf es besonderer Mechanismen, um einen ausfallsicheren Betrieb bspw. durch redundant ausgelegte Server zu sichern.
- **Integrität:** Darüber hinaus muss die Unverfälschtheit und Vertrauenswürdigkeit von Informationen und Daten durch die

[3] Vgl. Fraunhofer AISEC (2009): Cloud Computing-Sicherheit. Schutzziele, Taxonomie, Marktübersicht.

8

Collaboration-Lösung sichergestellt werden. So muss gewährleistet sein, dass kein externes System oder Angreifer Manipulationen vornehmen kann, bspw. um Schadsoftware wie Viren, Würmer oder Trojaner in die Unternehmens-IT einzuschleusen.

- **Authentizität:** Last, but not least muss eine eindeutige Identifikation bzw. Zuordnung jedes Nutzers garantiert sein. Dies ist vor allem im Support-Fall essenziell, wenn Dritte durch einen Fernzugriff Einblick in und Zugang auf gesamte Dateisysteme erlangen. So muss u. a. sichergestellt sein, dass kein Teilnehmer Informationen im Namen eines anderen erstellen bzw. vermitteln kann. Dies ist eine Schlüsselanforderung, die i. d. R. mit digitalen Signaturen, Sicherheitstoken oder Passwörtern sichergestellt wird.

Es gibt eine Vielzahl an Bedrohungen: Spoofing, Manipulationen, Sniffing, Denial of Service-Attacken …

Es besteht eine Vielzahl an ernsthaften Bedrohungen, die diese Schutzziele gefährden können. Dazu zählt Folgendes:

- Sog. **Spoofing**-Angriffe, bei denen Personen oder Systeme eine Zugriffsberechtigung vortäuschen, indem Daten verändert und Authentifizierungs- und Identifizierungsverfahren untergraben werden.
- **Manipulationen** zielen auf die vorsätzliche Verfälschung von Daten, Programmen oder Systemen. Zum Beispiel schalten sich bei Man in the Middle-Attacken Systeme oder Personen zwischen die Kommunikationspartner, sodass unberechtigte Dritte die vollständige Kontrolle über den Datenverkehr haben.
- Bei Angriffen zur **Informationsgewinnung** wie dem „Sniffing“ werden gezielt vertrauliche Informationen wie Zugriffsrechte oder Sicherheitsschwachstellen ausspioniert.
- **Denial of Service-Angriffe** (DoS) zielen darauf, die Collaboration-Lösung dienstunfähig zu machen, indem die vorhandenen Ressourcen, bspw. der Kommunikationsserver, durch massenhafte Anfragen überlastet werden.

Nicht nur technische, sondern auch organisatorische Maßnahmen wie Mitarbeitersensibilisierung und -schulung sind notwendig.

Sicherheitsrisiken können sowohl von gezielten Hacker-Angriffen mit ausgefeilten Techniken als auch von Mitarbeitern mit einem mangelnden Sicherheitsverständnis ausgehen. Deswegen müssen neben **technischen** auch **organisatorische Maßnahmen** ergriffen werden, z. B. um Mitarbeiter hinsichtlich möglicher Sicherheitsrisiken zu sensibilisieren und zu schulen.

9

Einen Überblick über die erläuterten Schutzziele und Gefahren gibt folgende Abbildung:

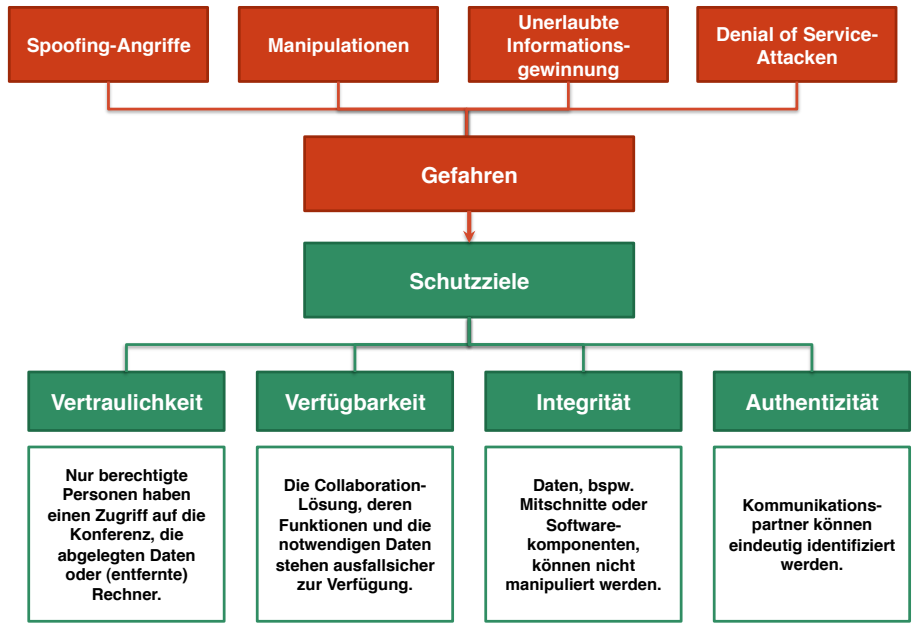

Abb. 3: Schutzziele und Gefahren im Überblick

FAZIT

- Der Einsatz von Collaboration-Lösungen vereinfacht die Zusammenarbeit signifikant, ist aber mit nicht zu unterschätzenden Sicherheitsrisiken verbunden.
- Zahlreiche Gefahren wie Spoofing, Manipulationen, Sniffing oder Denial of Service-Attacken gefährden die Sicherheit unternehmenssensibler Informationen und Daten.
- Bei der Auswahl einer Collaboration-Lösung sollte berücksichtigt werden, wie verschiedene Schutzziele adressiert werden, um die Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität der Kommunikation sicherzustellen.
- Aber nicht nur technische Maßnahmen sind wichtig, sondern auch organisatorische, wie die regelmäßige Schulung und Sensibilisierung von Mitarbeitern.

10

3. SICHERHEIT DER ARCHITEKTUR

OpenScape Web Collaboration basiert auf einer **Client-Server-Architektur**. Die **Server**software stellt die Collaboration-Funktionalitäten zur Verfügung, die dann über die **Web Collaboration Software** (Client) vom Anwender genutzt werden können. Die Einrichtung und Verwaltung der Konferenzen erfolgt dabei über ein webbasiertes **Portal**. Wie diese Komponenten zusammenspielen und dabei verschiedene Sicherheitsaspekte adressieren, zeigen die folgenden Abschnitte.

OpenScape Web Collaboration basiert auf einer Client-Server-Architektur.

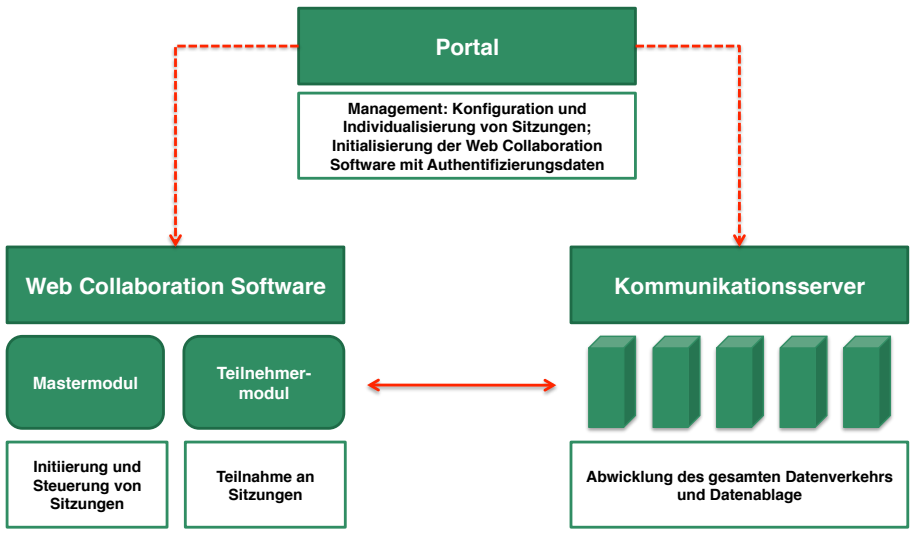

Abb. 4: Architektur von OpenScape Web Collaboration

3.1. Web Collaboration Software

Ein Auslesen und Manipulieren der Web Collaboration Software, bspw. um Schadsoftware zu verbreiten, ist nur sehr schwer möglich.

Bei OpenScape Web Collaboration werden zwei Versionen unterschieden, die sowohl für **Windows-** als auch für **Macintosh**-Rechner zur Verfügung stehen:

- das **Master-** bzw. **Moderatorenmodul**, welches die erworbene Lizenz beinhaltet und als Sitzungsinitiator dient;
- das **Teilnehmer-** bzw. **Kundenmodul,** das zur Konferenz oder Fernwartung auf den verschiedenen Endgeräten der teilnehmenden Anwender gestartet wird.

Sicherheitsrelevant ist vor allem, dass die Web Collaboration Software nicht durch Dritte manipuliert werden kann und keine sensiblen Informationen wie Lizenzdaten abgegriffen werden können. Bei OpenScape Web Collaboration sind die **ausführbaren Dateien** (Binaries) der Teilnehmer- und

Mastermodule **signiert** und damit **vor Manipulationen,** bspw. durch Schadsoftware, **sehr gut geschützt.** So war auch ein Dekompilieren, d. h. Auslesen des Codes, im praktischen Test nicht möglich.

Zudem werden über das Portal in beide Software-Versionen Informationen zu den genutzten Kommunikationsservern eingefügt. Somit können später nur vordefinierte Server angewählt werden, sodass ein **Abhören** durch unberechtigte (Server) **erschwert** wird.

Mastermodul

Eine zentrale Steuerung und Kontrolle ist nur über das Mastermodul möglich.

Konferenzen und Fernwartungssitzungen können nur über ein Mastermodul gebucht und gestartet werden, da es den **Lizenzschlüssel** enthält, der vom Portal vergeben und vom Kommunikationsserver abgefragt wird. Damit werden Mastermodule **eindeutig authentifiziert**, sodass nur Teilnehmer mit einer gültigen Lizenz Konferenzen und Fernwartungssitzungen buchen und starten können.

Das Mastermodul sollte, sofern nicht über die Benutzerverwaltung geschützt, auf keinen Fall an Dritte weitergegeben und immer in der aktuellsten Softwareversion verwendet werden.

Auch die **Konfiguration** der Konferenzen (also das Verändern der Konferenzparameter), das Einladen von Teilnehmern und die Rechtevergabe sind nur über das Mastermodul möglich. Dazu gehört bspw. das Freigeben von Bildschirminhalten oder das Weiterreichen dieser Freigabe an andere Teilnehmer. Somit können Konferenzteilnehmer ihren Desktop erst mit anderen teilen, wenn die Freigabe über den Moderator mit dem Mastermodul erfolgt. Die Steuerung und **Kontrolle** der Konferenz liegt damit **vollständig** in der Hand des **Initiators**. Allerdings kann jeder, der ein Mastermodul besitzt, Konferenzen starten und konfigurieren. Daher ist dringend zu empfehlen, das Mastermodul zusätzlich über die **Benutzerverwaltung** zu schützen. Andernfalls sollte das Mastermodul **auf keinen Fall an Dritte weitergegeben** werden. Darüber hinaus ist es ratsam, das Mastermodul immer in der **aktuellsten Softwareversion** zu nutzen. Die Verwendung einer Mindestversionsnummer kann über den Kommunikationsserver **erzwungen** werden.

Teilnehmermodul

Browserbasierter Client unterstützt plattformübergreifende Nutzung

Das Teilnehmermodul dient Eingeladenen zur Einwahl in **Konferenzen und Fernwartungssitzungen.** Grundsätzlich bestehen bei Konferenzen zwei verschiedene Optionen: Teilnehmer können sich über eine **ausführbare Datei** (.exe) oder über einen **Link** zu einer **Website** einwählen.

Bei Teilnahme mittels Webclient können Konferenzen unabhängig vom Betriebssystem des Endgerätes genutzt werden. OpenScape Web Collaboration unterstützt alle **gängigen Browser,** darunter Internet Explorer, Firefox, Chrome und Safari. Dabei kann der Webclient **Flash**- oder **JavaScript**-basiert sein, wobei Flash vor allem Vorteile hinsichtlich der Usability, bspw. Zugriff auf die eigene Webcam, bietet. Bei der webbasierten Nutzung sollte stets darauf geachtet werden, dass immer die **aktuellsten Browserversionen**, mit entsprechenden **Sicherheitsupdates,** im Einsatz sind.

3.2. Kommunikationsserver

Der Kommunikationsserver ist eine zentrale, sicherheitskritische Komponente.

Der Kommunikationsserver ist die **zentrale** und damit **sicherheitskritischste Komponente** der Collaboration-Lösung: Zum einen wird über ihn der gesamte Datenverkehr während einer Konferenz abgewickelt, zum anderen werden hier Konferenzdaten und geteilte Dokumente verschlüsselt abgelegt.

Eine eindeutige Authentifizierung erfolgt über die Nutzerlizenzen.

Bei Buchung bzw. Start einer Konferenz nimmt der Kommunikationsserver einen **Abgleich** von der im Mastermodul integrierten und der vom Portal übermittelten **Nutzerlizenz** vor. Erst nach erfolgreicher **Authentifizierung** können über das Mastermodul weitere Teilnehmer eingeladen werden. Sollte ein Mastermodul doch einmal in die falschen Hände geraten sein, kann dies gesperrt werden, indem die Lizenzen auf den Kommunikationsservern entfernt werden. Dies ist jedoch nicht nötig, wenn die Benutzerverwaltung bereits aktiviert ist, sodass sich kein Nutzer ohne gültige Log-in-Daten einwählen kann. Die Benutzerverwaltung kann auch jederzeit nachträglich aktiviert werden.

Mehrfach ausgelegte Server sichern eine hohe Verfügbarkeit der cloud-basierten Lösung.

Beim Start einer Konferenz über die **cloud-basierte** Lösung wird vom Mastermodul der Kommunikationsserver bestimmt, der aktuell die **höchste Verfügbarkeit** aufweist. Derzeit befinden sich **44 Kommunikationsserver**[4] in der Cloud-Infrastruktur von Siemens Enterprise Communications/FastViewer. Solange mindestens einer der Server funktionstüchtig und erreichbar ist, können Konferenzen durchgeführt werden. Denn der Ausfall einzelner Server führt nicht zum Ausfall des gesamten Systems. Damit ist eine **hohe Verfügbarkeit und Ausfallsicherheit** der cloud-basierten Lösung sichergestellt.

[4] Stand: September/Oktober 2011

Der Austausch von hochsensiblen Unternehmensdaten kann über die cloud-basierte Lösung aus datenschutzrechtlicher Sicht problematisch sein.

Allerdings befinden sich bei der cloud-basierten Lösung die Server in Rechenzentren von verschiedenen Providern, teils in unterschiedlichen Ländern. Dies kann beim Austausch hochsensibler Unternehmensdaten aus datenschutzrechtlicher Sicht problematisch sein. Siemens Enterprise Communications plant jedoch die Option, im cloud-basierten Modell ausschließlich **europäische** oder **deutsche Rechenzentren** nutzen zu können. Darüber hinaus ist es schon jetzt möglich, die Kommunikationsserver als **dedizierte Hosting-Lösung** zu nutzen, bei der die Kommunikationsserver **exklusiv,** für nur einen Kunden, bereitgestellt werden.

Wenn ein Unternehmen einen **eigenen Kommunikationsserver on-premise** betreibt, erfolgt der Verbindungsaufbau zu den definierten unternehmensinternen Servern. Auch hier empfiehlt es sich, die Ausfallsicherheit durch redundant ausgelegte Server abzusichern.

3.3. Portal

Über das Portal erfolgt die gesamte Verwaltung der Collaboration-Lösung: alles was Konfiguration, Individualisierung und auch Sicherheitseinstellungen betrifft.

OpenScape Web Collaboration wird vollständig über ein webbasiertes Portal verwaltet. Hier erfolgt zum einen die **Konfiguration** und **Individualisierung** von Konferenzen und Fernwartungssitzungen, zum anderen werden hier alle **Nutzerdaten**, bspw. die Lizenznummer oder gebuchte Editionen, sowie Informationen zu den genutzten Kommunikationsservern gespeichert und verwaltet.

Bei der Installation dient das Portal vor allem dem **Erstellen** und dem **Download** der **Web Collaboration Software**. Über diese wird die Lösung (vor-) konfiguriert, d. h. es werden Standardeinstellungen und Funktionsumfang festgelegt und in die Master- und Teilnehmermodule als eine ausführbare Datei integriert. Hierzu zählen auch sämtliche **Sicherheitseinstellungen**, bspw. die Vergabe zur Berechtigung von Desktop-Sharing oder die (De-) Aktivierung von Videoaufzeichnungen. Dabei sind die erstellten Master- und Teilnehmermodule fest an die über das Portal getätigten Einstellungen gebunden, sodass die **zentrale Umsetzung** von **Compliance-Vorschriften** möglich ist.

Das Festlegen von Profilen unterstützt die zentrale Durchsetzung von Compliance-Vorschriften.

Durch das Konzept der Master- und Teilnehmermodule können über das Portal für **unterschiedliche Anwendungsszenarien** bzw. Nutzergruppen verschiedene Profile mit bestimmten Sicherheitseinstellungen zusammengestellt werden. Für Unternehmen empfiehlt es sich, die Sicherheitsanforderungen verschiedener Nutzergruppen vorab zu

14

Das Portal stellt keinen Single Point of Failure dar.

analysieren, um diese dann über die Portaleinstellungen abzubilden. So können sich die Sicherheitsanforderungen zwischen einem Marketing-Webcast, einem Management-Meeting und dem Support-Fall, bei dem der Zugriff auf das gesamte Dateisystem möglich ist, erheblich unterscheiden.

Sofern keine Konfigurationsänderungen notwendig sind, wird das Portal für die weitere Nutzung (bspw. für den Verbindungsaufbau) nicht mehr benötigt. Vor diesem Hintergrund stellt das Portal **keinen Single Point of-Failure** dar: Sollte es zu einem Ausfall des Portals kommen, können problemlos weiterhin Konferenzen stattfinden.

Aufgrund der enthaltenen sensiblen Daten, bspw. Angaben über die Kommunikationsserver, stellt das Portal für Dritte ein **interessantes Angriffsziel** dar. Bei OpenScape Web Collaboration erfolgt die Zugangskontrolle zum Portal über einen Benutzernamen bzw. eine Lizenznummer und ein entsprechendes achtstelliges Kennwort.[5] Die gesamte Kommunikation erfolgt dabei **SSL-verschlüsselt**.

FAZIT

- Die Rollenverteilung aller Architekturkomponenten (Web Collaboration Software, Server und Portal) ist klar festgelegt und stellt insgesamt eine elegante Lösung dar, um potenzielle Gefahren auszuschließen.
- Durch das Konzept der Master- und Teilnehmermodule (in Verbindung mit dem Portal) ist sichergestellt, dass nur (authentifizierte) Nutzer, die tatsächlich eine Lizenz innehaben, Konferenzen und Fernwartungssitzungen aufsetzen und konfigurieren sowie Rechte an andere weitergeben können. Durch die Integration der Serverlisten in die Web Collaboration Software ist eine Manipulation von außen weitestgehend ausgeschlossen.
- Darüber hinaus sind die ausführbaren Dateien (Binaries) der Teilnehmer- und Mastermodule signiert und damit vor Manipulationen sehr gut geschützt. So war auch ein Dekompilieren, d. h. Auslesen des Codes, im praktischen Test nicht möglich.

[5] Zugang zum Portal und deren Sicherheitsmechanismen waren nicht Teil der Sicherheitsanalyse, da das Portal nicht in die eigentliche Kommunikation involviert ist. Die Sicherheitsanalyse erstreckte sich auf die wesentlichen Infrastrukturkomponenten (Server und Clientmodule) und deren Services.

15

- Die zentrale Steuerung einer Konferenz erfolgt über das Mastermodul, wodurch die Kontrolle immer beim Initiator liegt. Allerdings enthält diese Komponente die Nutzerlizenz, und jeder, der dieses Modul besitzt, kann eine Konferenz starten und Sicherheitsparameter verändern. Das Mastermodul sollte deshalb unbedingt über die Benutzerverwaltung geschützt werden.
- Bei der cloud-basierten Lösung sichern mehrfach ausgelegte Server eine hohe Verfügbarkeit ab. Auch beim On-premise-Betrieb empfiehlt es sich, die Ausfallsicherheit durch redundant ausgelegte Server abzusichern.
- Über das webbasierte Portal erfolgen Sicherheits- und Funktionseinstellungen sowie eine Initialisierung der Web Collaboration Software mit Authentifizierungsdaten, sodass Compliance-Vorschriften zentral umgesetzt werden können. Das Portal selbst dient vor allem der Konfiguration und stellt vor diesem Hintergrund keinen Single Point of Failure dar.

4. NUTZERAUTHENTIFIKATION UND TEILNEHMERVERWALTUNG

4.1. Nutzerauthentifikation

Die Authentifikation der Nutzer erfolgt über eine sitzungsspezifische Sitzungsnummer.

Bei den Konferenzlösungen von OpenScape Web Collaboration wird die Authentifikation über eine 5-stellige, sitzungsspezifische **Sitzungsnummer** (Session ID), die beim Start einer Konferenz automatisch vom Mastermodul erzeugt wird, und einem optional zu vergebenden Passwort realisiert. Beim Eigenbetrieb von OpenScape Web Collaboration können auch längere Session IDs verwendet werden. Grundsätzlich gilt: Je länger die Session ID, umso geringer ist die Wahrscheinlichkeit, dass sich nicht geladene Teilnehmer über die Brute Force-Methode[6] Zutritt verschaffen.

Zusätzlich sollte immer der Passwortschutz mit einer hinreichenden Passwortkomplexität verwendet werden.

Unternehmen sollten darüber hinaus immer den **optional** vorhandenen **Passwortschutz** verwenden. Über die Benutzerverwaltung besteht die Möglichkeit, Passwortkomplexität und -länge zu erzwingen. (Passwörter sollten immer länger als sechs Zeichen sein und neben Groß- und Kleinbuchstaben auch Sonderzeichen und Ziffern enthalten.) Da das Passwort mit der Session ID jedoch nur im Klartext per E-Mail versendet wird, könnte durch falsches Weiterleiten ein unbefugter Zugriff erfolgen, da keine dedizierte Clientauthentifizierung erfolgt. Hier ist dringend zu empfehlen, E-Mails zu verschlüsseln und nur einem kleinen Nutzerkreis zukommen zu lassen.

Alternativ kann die Nutzerauthentifikation auch über das Portal und Active Directory erfolgen.

Die Nutzerauthentifikation kann **alternativ** zu Session ID und Passwort **lokal** über das **Portal** oder über ein vorhandenes **Active Directory** – jeweils auf Benutzer- oder Gruppenebene – erfolgen. Auch eine Kombination aus Active Directory-Integration und zusätzlicher Benutzerverwaltung ist möglich. Der jeweils verwendete Authentifizierungsmechanismus kann jedoch grundsätzlich projekt- bzw. **kundenspezifisch angepasst** werden, um ein höheres Sicherheitsniveau zu gewährleisten, bspw. durch Ergänzung per Smartcard. Die entsprechende Umsetzung ist allerdings abhängig vom jeweiligen Anwenderunternehmen und nicht Basisbestandteil der Lösung.

[6] Methode, um durch Ausprobieren aller möglichen (Kombinations-) Fälle die Sitzungsnummer zu ermitteln.

Bei OpenScape Web Collaboration wird zusätzlich zu diesen zwei Authentifikationsoptionen die im **Mastermodul** integrierte **Nutzerlizenz** geprüft. Es handelt sich dabei um eine 10-stellige Nummer, die mit einem dedizierten Datenbanksystem abgeglichen wird. Die Lizenzprüfung erfolgt nach Aushandlung des initialen 256-Bit-AES-Schlüssels und vor Aushandlung des (zweiten) Sitzungsschlüssels, sodass die entsprechenden Informationen verschlüsselt und sicher übermittelt werden. Als Anti-Bruteforcing-Maßnahme wird darüber hinaus bei jedem fehlgeschlagenen Versuch das integrierte Time-out verdoppelt.

Insgesamt kann mit den dargestellten Sicherheitsmechanismen unter Berücksichtigung der Empfehlungen eine sehr sichere Authentifizierung erreicht werden.

4.2. Teilnehmerverwaltung

Logfiles liefern ein Indiz über Teilnehmer, sind jedoch kein Sicherheitsfeature.

Wird eine Konferenz abgehalten, werden in einem **Logfile** der vom Teilnehmer frei wählbare Log-in-Name, die Session ID, die Teilnehmeranzahl, die Lösungsversionsnummer, der Windows-Anmeldename, Hostnamen, IP-Adressen, Freitextpositionen und ein Zeitstempel protokolliert. Diese Logfiles können bei der cloud-basierten Lösung über das Kundenportal und bei einer On-premise-Lösung über ein eigenes Tool eingesehen und ausgewertet werden. Dies liefert ein **Indiz** dafür, wer an einer Konferenz teilgenommen hat; die eindeutige Zuordnung zu einem Benutzer ist jedoch nicht möglich. Nur bei einer On-premise-Installation werden nach jeder Sitzung auf dem Kommunikationsserver Logfile-Nachrichten abgelegt, sodass die Teilnahme auf Nutzerebene einsehbar ist.

Die **Benutzerverwaltung** selbst kann nur vom Lizenzinhaber über das Mastermodul **aktiviert** werden, sodass Moderatoren diese zwar einsehen, aber nicht aufrufen können. Die Rollenverwaltung wird über den Kommunikationsserver abgewickelt und kann über das Mastermodul eingerichtet werden. Hier erfolgt die Aufteilung von Rechten, sodass sicherheitskritische Einstellungen nur von einem Administrator implementiert und verändert werden können.[7]

[7] Das Portal war nicht Teil der Sicherheitsanalyse.

18

FAZIT

- Mit den vorhandenen Sicherheitsmechanismen kann unter Berücksichtigung der Empfehlungen insgesamt eine sehr sichere Authentifizierung erreicht werden.
- Zusätzlich zur mindestens 5-stelligen Session ID sollte immer der optional vorhandene Passwortschutz verwendet werden, mit einer hinreichend großen Passwortkomplexität. Werden die Log-in-Daten via E-Mail versandt, sollten diese bspw. durch Verschlüsselung gesichert werden.
- Die Identität des Konferenzinitiators wird sicher über die im Mastermodul integrierten Lizenznummern überprüft. Verschlüsselung und Time-outs verhindern Angriffe wie Man in the Middle-Attacken und Bruteforcing.
- Die Aufzeichnung von nutzerspezifischen Daten über Logfiles gibt einen Hinweis auf die tatsächliche Teilnahme von Nutzern; eine eindeutige Zuordnung ist jedoch nicht möglich.
- Die Benutzerverwaltung wird über den Kommunikationsserver abgewickelt und kann über das Mastermodul eingerichtet werden, sodass sicherheitskritische Einstellungen nur von einem Administrator konfiguriert werden können.

5. VERBINDUNGSAUFBAU UND -SICHERHEIT

Für die Sicherheit der Collaboration-Lösung ist das zugrunde liegende Konzept zum Verbindungsaufbau und Datenaustausch zentral. Denn darüber wird die **Vertraulichkeit** der **Kommunikation** und der **abgelegten Daten** sichergestellt. So muss verhindert werden, dass unerwünschte Dritte die Gespräche während einer Konferenz abhören (bspw. bei der Nutzung eines offenen WLANs) oder einen unbefugten Zugriff auf die (möglicherweise) abgelegten Daten erlangen können, z. B. auf Präsentationen oder gemeinsam bearbeitete Dateien.

5.1. Absicherung der Kommunikationswege

Verbindungsaufbau – Firewalls & Ports

OpenScape Web Collaboration unterstützt gängige Ports, sodass keine sicherheitskritischen Umstellungen und Anpassungen an der Firewall notwendig sind.

Um Webkonferenzsysteme und Fernwartungsanwendungen generell nutzen zu können, müssen auf Unternehmensseite bei der Firewall **Ports freigeschaltet** sein. Allerdings bestehen umso mehr **potenzielle Angriffspunkte**, je mehr Ports für eine Anwendung offen gehalten werden müssen. OpenScape Web Collaboration unterstützt neben einem in der Firewall nicht immer freigegebenen Weg über den Port 5000 (TCP) auch die Kommunikation über **gängige Ports** wie 443 (HTTPS) und 80 (HTTP), sodass **keine sicherheitskritischen Umstellungen** und **Anpassungen** auf Seiten der Firewall notwendig sind.

Der Port 5005 kann optional gewählt und im Kundenportal aktiviert werden, wenn sich die beteiligten Systeme im selben Unternehmensnetz (LAN) befinden, und ist eine „proprietäre“ Lösung. Welcher der genannten Ports letztlich verwendet wird, ist jedoch nicht sicherheitsrelevant, da die **Verbindungen** in jedem Fall mit dem 256-Bit-AES-Standard **verschlüsselt** erfolgen. Allerdings ist zu empfehlen, den **Port 443** (HTTPS) zu nutzen, da die Datenpakete von gängigen Proxys nicht analysiert werden, wodurch keine Latenzzeiten entstehen, die sich nachteilig auf die Performance der Collaboration-Lösung auswirken. Unternehmen, die den Kommunikationsserver on-premise betreiben, können selbst festlegen, welche Ports verwendet werden sollen.

20

Die Kommunikation zwischen Infrastrukturkomponenten ist AES-verschlüsselt.

Verbindungssicherheit – Protokolle & Zertifikate

Da bei webbasierten Collaboration-Lösungen das Internet genutzt wird, muss die Datenverbindung durch verschiedene, komplex ineinander greifende Maßnahmen gesichert werden. Bei OpenScape Web Collaboration ist die Kommunikation zwischen den Architekturkomponenten (Web Collaboration Software und Server) mit dem **AES-256-Algorithmus** verschlüsselt. Da es sich hierbei um einen symmetrischen Schlüssel handelt, sind dessen **sicherer Austausch** zwischen den beteiligten Kommunikationspartnern sowie dessen **sichere Verwaltung** (Verwahrung und Schutz gegen unberechtigte Zugriffe) von immanenter Bedeutung für die Sicherheit der gesamten Lösung. Denn über **Man in the Middle-Attacken** sind solche Sicherheitsmaßnahmen grundsätzlich aushebelbar.

Zuerst findet eine eindeutige Identifizierung statt, erst danach werden die Sitzungsschlüssel ausgetauscht.

Bei OpenScape Web Collaboration werden für jede (neue) Konferenz oder Fernwartung **dediziert Sitzungsschlüssel** generiert, ausgetauscht und für die Sitzung verwendet. Dabei werden die Schlüssel in einem zweistufigen Verfahren ausgehandelt:

- In einem ersten Schritt findet eine **Identifikation und Authentifizierung aller Kommunikationspartner** statt. Dabei kommen verschiedene Verschlüsselungsmechanismen und Signaturen zum Einsatz. Auf diese Weise ist zum einen die Authentizität des Kommunikationsservers vollständig sichergestellt und zum anderen die wirksame Abwehr sog. Man in the Middle-Attacken.
- Erst im zweiten Schritt wird zwischen Teilnehmer- und Mastermodul über den „validierten“ Kommunikationsserver der eigentliche **Sitzungsschlüssel** ausgetauscht, mit dem die Verschlüsselung der **Nutzdaten** erfolgt.

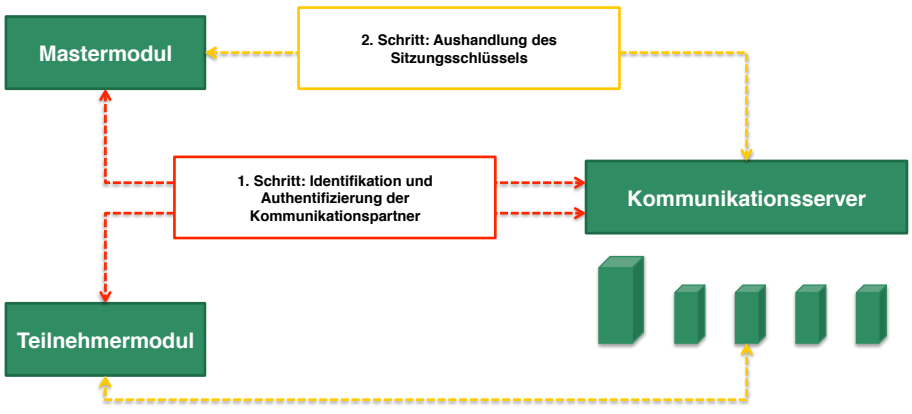

Abb. 5: Grobkonzept des Kommunikationsaustauschs

Die eingesetzten Verschlüsselungsverfahren, Schlüssellängen und Protokolle sind technisch auf dem aktuellsten Stand.

Die theoretischen und praktischen Analysen zeigten, dass die eingesetzten **Verschlüsselungsverfahren, Schlüssellängen und Protokolle** technisch auf dem **aktuellsten Stand** sind. Darüber hinaus werden über den **Secure Connect Service** die Datenpakete auf dem Kommunikationsserver lediglich durchgereicht, wodurch eine **End-to-end-Verschlüsselung** gegeben und damit eine nicht autorisierte Einsichtnahme unterbunden wird. Wenn kein eigener Server on-premise installiert ist, erfolgt die Verbindung automatisch über die von Siemens Enterprise Communications angebotene Cloud-Lösung.

Zusätzlich werden auf den **Siemens Enterprise Communications-eigenen Kommunikationsservern** eine Reihe von **Sicherheitsmaßnahmen** umgesetzt: Auf den gehärteten Servern sind ausschließlich Collaboration-Services der Lösung aktiv, für die keine Schwachstellen bekannt sind; hinzu kommt die Verdoppelung des Time-outs bei ungültigen Log-in-Versuchen und nicht zuletzt die Verteilung der Kommunikationsserver auf mehrere Rechenzentren.

Bei einem vertrauenswürdigen Kommunikationsserver liegt insgesamt ein **wirkungsvolles Konzept** zugrunde, um **Man in the Middle-Attacken** abzuwehren. Sollten allerdings die Kommunikationsserver on-premise betrieben werden, liegt es in der Verantwortung des Unternehmens selbst, das Sicherheitsniveau der Kommunikationsserver sicherzustellen.

OpenScape Secure Advisor – Aufbau einer direkten Verbindung

Im Support-Fall sollte nach Möglichkeit die Autolock-Funktion genutzt werden.

Speziell für den Support-Fall besteht die Möglichkeit, eine 1:1-Beziehung zwischen Teilnehmer- und Mastermodul festzulegen. Sobald sich Kunde und Support eingeloggt haben, wird die aktuelle Session für weitere Teilnehmer gesperrt. Diese **Autolock-Funktion** ist über das Kundenportal aktivierbar und aus Sicherheitsaspekten immer zu empfehlen.

5.2. Datenhaltung und -verarbeitung

Die Datenhaltung und -verarbeitung ist auf dem Server hinreichend gesichert.

Der Kommunikationsserver ist ein interessantes Angriffsziel, da auf ihm eine Vielzahl an **Sitzungsnummern** und **Passwörtern** gespeichert werden. Daher kommt Sicherheitsmaßnahmen hier eine besonders hohe Bedeutung zu. Die Analysen zeigten Folgendes:

- Benutzerdaten wie Sitzungsnummer und Passwort werden nicht langfristig im Dateisystem oder einer Datenbank gespeichert, sodass kein nachträgliches Auslesen stattfinden kann.

- Bei der Active Directory-Integration wird das Domänenpasswort nicht gespeichert, und damit ist kein Zugriff auf die dahinterliegenden Ressourcen möglich.
- Nur bei direktem Zugriff auf den Kommunikationsserver war eine unautorisierte Extraktion des Sitzungsschlüssels und des Kennwortes möglich. Bei einer on-premise betriebenen Lösung muss der Zugang zum Server durch entsprechende Maßnahmen wie Passwortschutz abgesichert werden.

Damit ist die Datenhaltung und -verarbeitung auf dem Server hinreichend gesichert.

Installationsfreiheit sichert rückstandsfreie Nutzung der Softwareclients

Ein weiterer, wichtiger Aspekt ist die **rückstandsfreie Nutzung** der Master- und Teilnehmermodule. Diese sind, abgesehen vom Remote-Client, ausführbare Dateien, bei denen keine Software installiert wird. Auf diese Weise kann niemand nach Abschluss einer Konferenz auf die Konferenzdaten zugreifen und bei der Nutzung der Web Collaboration Software werden keinerlei Dateien und Einstellungen des genutzten Rechners verändert.

FAZIT

Insgesamt liegt OpenScape Web Collaboration ein wirkungsvolles Sicherheitskonzept zugrunde:

- Es werden gängige Ports unterstützt, sodass keine sicherheitskritischen Umstellungen und Anpassungen der Firewall notwendig sind.
- Die Kommunikation zwischen den Architekturkomponenten (Web Collaboration Software und Server) ist mit dem 256-Bit-AES-Algorithmus verschlüsselt. Zuerst findet eine eindeutige Identifizierung der Master- und Teilnehmermodule statt, erst danach werden die Sitzungsschlüssel ausgetauscht.
- Die eingesetzten Verschlüsselungsverfahren, Schlüssellängen und Protokolle sind technisch auf dem aktuellsten Stand.
- Da die Datenpakete über den „Secure Connect Service“ auf dem Kommunikationsserver lediglich durchgereicht werden, liegt eine Ende-zu-Ende-Verschlüsselung vor, die durch eine Reihe zusätzlicher Maßnahmen auf Serverseite abgesichert wird.

23

- Für Support-Fall sollte nach Möglichkeit unbedingt die Autolock-Funktion genutzt werden.
- Bei der Web Collaboration Software handelt es sich um ausführbare Dateien, deren Betrieb rückstandslos erfolgt. Dadurch werden keinerlei Dateien und Einstellungen des genutzten Rechners verändert.

6. COLLABORATION-FUNKTIONEN

OpenScape Web Collaboration bietet **abhängig** von der **gebuchten Edition** verschiedene Collaboration-Funktionen, die in bestimmten Situationen sicherheitskritisch sein können.

6.1. OpenScape Instant Meeting – Konferenzfunktionen

Aufzeichnung von Videos

Sitzungsmitschnitte sind eine nützliche Funktion für die eigene Dokumentation, eignen sich jedoch (noch) nicht für die revisionssichere Archivierung.

Sitzungsmitschnitte können von allen Teilnehmern lokal auf den Rechnern aufgezeichnet werden und sind eine nützliche Funktion für eigene Dokumentationszwecke. Wird von einem Teilnehmer eine Aufzeichnung gestartet, werden alle anderen Teilnehmer darüber automatisch informiert, sodass **keine unautorisierten Mitschnitte** möglich sind. Im praktischen Sicherheitstest zeigte sich jedoch, dass die aufgezeichneten Videodateien manipulierbar und damit für eine **revisionssichere Archivierung (noch) nicht geeignet** sind. Bis eine neue Version der Web Collaboration Software diese Sicherheitsfunktion unterstützt, sollten **zusätzliche Maßnahmen** ergriffen werden, um Manipulationen zu erschweren. Zum einen sollte vorkonfiguriert werden, dass Sitzungsmitschnitte **automatisch gestartet** und **beendet** werden, zum anderen sollte die Ablage der Mitschnitte nur auf **revisionssicheren Speichersystemen** erfolgen, bei denen nur einmalige Schreibrechte bestehen.

Dateiablage

Um die Gefahr eines unerlaubten Zugriffs auf abgelegte Dokumente zu beschränken, sollten Konferenzdaten nur an einen kleinen Nutzerkreis weitergegeben werden.

Alle Konferenzteilnehmer können Dateien wie Präsentationen oder Textdokumente auf dem Kommunikationsserver ablegen, um sie mit anderen während einer Sitzung zu teilen. Die abgelegten Dateien werden mit dem gemeinsamen Sitzungsschlüssel **codiert**, sodass nur eingeladene Konferenzteilnehmer einen Zugriff darauf haben. Dabei ist der **Austausch des Sitzungsschlüssels sicher** verschlüsselt. Allerdings gilt auch hier, dass durch eine **fehlgeleitete E-Mail** auch nicht eingeladene Dritte einen Zugriff auf die Datenablage erhalten. Deswegen sollten die **Konferenzdaten** nur an einen **kleinen Nutzerkreis** weitergegeben und ggf. über **verschlüsselte E-Mails** gesendet werden. Darüber hinaus sollte der Sitzungsraum abgesperrt werden, sobald sich alle Teilnehmer eingewählt haben. Bei sensiblen Konferenzthemen sollten die Einwahldaten zudem nur einmalig verwendet werden. Nach einer Konferenz werden alle abgelegten

Daten automatisch gelöscht, sodass kein Teilnehmer mehr darauf zugreifen kann.

Portmapper

Der Portmapper ist keine direkte Collaboration-Funktion, sondern dient dazu, die Firewall zu umgehen, um eine nachträgliche Anpassung der Filterregeln zu vermeiden. Dies ist eine sicherheitskritische Funktion, da mit dem Umgehen der Firewall vorgesehene Schutzmechanismen ausgeschaltet werden, und sollte daher nur in Ausnahmefällen eingesetzt werden. Der Portmapper kann nur vom Administrator über das Portal (de-) aktiviert werden.

6.2. OpenScape Secure Advisor – Support-Funktionen

Remote-Zugriff

Beim Remote-Zugriff hat der zu unterstützende Nutzer die volle Kontrolle über die Fernwartung – vorausgesetzt, er ist über die hier dargestellten Sicherheitsrisiken und -mechanismen informiert.

Im Remote-Modus, bei dem ein Rechner vollständig durch eine Fernwartung bedient werden kann, erfolgt der Zugriff vom Mastermodul aus über den Kommunikationsserver. Der (zu unterstützende) **Nutzer sieht** bei einer **aktiven Verbindung**, mit wem er verbunden ist und über welche Berechtigungen der andere verfügt. Darüber hinaus gibt es zwei **Kontrollmöglichkeiten**: Erstens kann die Zeit bis zum Zugriff auf einen entfernten Rechner beschränkt werden (Remoted Countdown); nach Ablauf der festgelegten Frist wird der Remote-Zugriff automatisch gestartet oder nicht. Zweitens kann der Remote-Zugriff jederzeit vom Client aus selbst über einen **Tastendruck gestoppt** (Per default F11) werden. Auch die jeweiligen Berechtigungen bzw. freigegebenen Bereiche lassen sich individuell festlegen und jederzeit erweitern oder einschränken. Somit hat der (zu unterstützende) Nutzer eine **volle Kontrolle über die Fernwartung** – sofern er über die entsprechenden Möglichkeiten informiert ist. Daher sollten Mitarbeiter, auf deren Rechner remote zugegriffen wird, hinreichend geschult und sensibilisiert werden.

Dateitransfer

Der Dateitransfer ist eine sicherheitskritische Funktion und sollte nur im Support-Fall eingesetzt werden, wenn ein hinreichend großes Vertrauen vorausgesetzt werden kann.

Für **Support**-Anwendungen können darüber hinaus mit dem Dateitransfer Dateien, bspw. Installationen oder Datenbankdateien, verschlüsselt ausgetauscht werden, dem der Nutzer **dediziert zustimmen** muss. Allerdings ist mit dieser Funktion im Unterschied zum Remote-Zugriff keine Ausführung von Programmen möglich. Bei dieser Funktion wird eine Verbindung zwischen Teilnehmer- und Mastermodul aufgebaut und alle

Aktivitäten werden in einer **Log-Datei** aufgezeichnet. Allerdings hat der „Zugreifende“ nach dem einmalig aktivierten Dateitransfer einen **Vollzugriff** auf das entfernte Dateisystem, d. h. die gleichen Rechte wie der angemeldete Benutzer. Dabei ist für den zu unterstützenden Nutzer zu jeder Zeit sichtbar, welche Aktionen der Remote-Nutzer auf seinem Rechner ausführt. Wenn zwischen den Teilnehmern jedoch kein **absolutes Vertrauen** vorausgesetzt werden kann, sollte nach Möglichkeit auf diese Funktion verzichtet werden. Alle Verwendungen außerhalb des Support-Falls sind als sehr kritisch einzustufen.

FAZIT

- Sitzungsmitschnitte sind eine praktische Funktion für die eigene Dokumentation, eignen sich jedoch (noch) nicht für die revisionssichere Archivierung. Um Manipulationen vorzubeugen, sollten Sitzungsmitschnitte automatisch gestartet und beendet sowie auf revisionssicheren Speichersystemen hinterlegt werden.
- Die Ablage von Dateien erfolgt sicher auf dem Kommunikationsserver. Um jedoch die Gefahr eines unerlaubten Zugriffs auf abgelegte Dokumente zu beschränken, sollten Konferenzdaten nur verschlüsselt und an einen kleinen Nutzerkreis weitergegeben werden.
- Beim Remote-Zugriff hat der zu unterstützende Nutzer die volle Kontrolle über die Fernwartung. Mitarbeiter, auf deren Rechner remote zugegriffen wird, sollten hinreichend geschult bzw. sensibilisiert werden.
- Der Dateitransfer ist eine sicherheitskritische Funktion und sollte nur im Support-Fall eingesetzt werden, wenn ein hinreichend großes Vertrauen zwischen den Parteien vorausgesetzt werden kann.

27

7. ZUSAMMENFASSUNG

Um die Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität der Kommunikation sicherzustellen, müssen webbasierte Collaboration-Lösungen in der Sicherheitsstrategie berücksichtigt werden.

Der Einsatz von webbasierten Collaboration-Lösungen vereinfacht die Zusammenarbeit signifikant, ist aber mit nicht zu unterschätzenden **Risiken** verbunden. Zahlreiche Gefahren wie Spoofing, Manipulationen, Sniffing oder Denial of Service-Attacken gefährden die Sicherheit **unternehmenssensibler Informationen** und **Daten**. Webkonferenz- und Fernwartungslösungen müssen daher in der **Sicherheitsstrategie** berücksichtigt werden, vor allem um die Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität der Kommunikation sicherzustellen.

Fraunhofer-Einrichtungen: Theoretische und praktische Sicherheitsanalyse von OpenScape Web Collaboration

Die **theoretischen** und **praktischen Sicherheitsanalysen** der **Fraunhofer-Einrichtungen** für Angewandte und Integrierte Sicherheit (**AISEC**) sowie für Systeme der Kommunikationstechnik (**ESK**) zeigten, dass mit den vorhandenen Sicherheitsmechanismen unter Berücksichtigung der hier gegebenen Empfehlungen eine **sichere Nutzung** von OpenScape Web Collaboration gewährleistet werden kann:

Das Architekturkonzept stellt insgesamt ein elegantes und wirksames Sicherheitskonzept dar.

Die **Rollenverteilung** aller **Architekturkomponenten** ist **klar festgelegt** und stellt insgesamt eine elegante Lösung dar, um potenzielle Gefahren auszuschließen. Durch das Konzept der **Master-** und **Teilnehmermodule** ist sichergestellt, dass nur **authentifizierte Nutzer** Konferenzen aufsetzen und konfigurieren können. Durch die Integration der Serverlisten in die Web Collaboration Software ist eine **Manipulation** von außen **weitestgehend ausgeschlossen**. Die **Web Collaboration Software** sind zudem **signiert**, was das Manipulieren des Quellcodes, bspw. mit Schadsoftware, so gut wie ausschließt. Darüber hinaus handelt es sich um **ausführbare Dateien**, deren Betrieb **rückstandslos** erfolgt, sodass bei Nutzung der Software keinerlei Dateien und Einstellungen des genutzten Rechners verändert werden.

Das Portal stellt keinen Single Point of Failure dar.

Über das **Portal** erfolgen Sicherheits- und Funktionseinstellungen sowie eine **Initialisierung der Clients** mit Authentifizierungsdaten, sodass **Compliance**-Vorschriften **zentral** umgesetzt werden können. Es dient vor allem der Konfiguration und stellt daher **keinen Single Point of Failure** dar.

28

Sicherheitsmechanismen beim Verbindungsaufbau sind technisch auf dem aktuellsten Stand.

Zur sicheren **Nutzerauthentifikation** stehen verschiedene Optionen zur Verfügung. Zusätzlich zur mindestens 5-stelligen **Session ID** sollte immer der optional vorhandene **Passwortschutz** verwendet werden. Neben Session ID und optionalem Passwort besteht die Möglichkeit, Nutzer **lokal** über das **Portal** und über **Active Directory** zu authentifizieren.

OpenScape Web Collaboration unterstützt für die Datenverbindung **gängige Ports**, sodass keine sicherheitskritischen Umstellungen der Firewall notwendig sind. Die Kommunikation zwischen den Architekturkomponenten (Web Collaboration Software und Server) ist **verschlüsselt**, wobei die Schlüssel in einem zweistufigen Verfahren ausgehandelt werden**:** Zuerst findet eine eindeutige Identifizierung der Web Collaboration Software statt, erst danach werden die Sitzungsschlüssel ausgetauscht. Da die Datenpakete auf dem **Kommunikationsserver** lediglich durchgereicht werden, liegt eine **Ende-zu-Ende-Verschlüsselung** vor, die durch eine Reihe zusätzlicher Maßnahmen auf Serverseite abgesichert wird. Dabei sind die eingesetzten **Verschlüsselungsverfahren**, **Schlüssellängen** und **Protokolle** technisch auf dem **aktuellsten Stand**.

Mehrfach ausgelegte Server sichern eine hohe Ausfallsicherheit ab.

Bei der cloud-basierten Lösung sichern **mehrfach ausgelegte Server** eine **hohe Verfügbarkeit** ab. Da diese sich jedoch in Rechenzentren von verschiedenen Providern, teils in verschiedenen Ländern, befinden, kann der **Austausch** von **hochsensiblen Unternehmensdaten** aus datenschutzrechtlicher Sicht **problematisch** sein. Es ist jedoch geplant, dem Anwender bei der cloud-basierten Nutzung die Option zu bieten, ausschließlich deutsche/europäische Server zu nutzen. Darüber hinaus ist es schon jetzt möglich, die Kommunikationsserver als **dedizierte Hosting-Lösung** zu nutzen, bei der die Systeme **exklusiv,** für nur einen Kunden, bereitgestellt werden. Auch beim On-premise-Betrieb empfiehlt es sich, die Ausfallsicherheit durch redundant ausgelegte Server abzusichern.

Neben technischen sind organisatorische Maßnahmen der Mitarbeiterschulung wichtig.

Aber nicht nur technische **Maßnahmen** sind wichtig, sondern auch **organisatorische** wie die regelmäßige Schulung und Sensibilisierung von Mitarbeitern. Dies ist vor allem bei der Nutzung von **Collaboration-Funktionen** elementar. So ist bspw. der Dateitransfer beim Fernzugriff eine sicherheitskritische Funktion, die nur im Support-Fall eingesetzt werden sollte, wenn ein hinreichend großes Vertrauen zwischen den Parteien vorausgesetzt werden kann.

8. ÜBER DEN AUFTRAGGEBER

SIEMENS

Siemens Enterprise Communications

Siemens Enterprise Communications, ein Gemeinschaftsunternehmen der Siemens AG und der Gores Group, blickt auf eine Geschichte von mehr als 160 Jahren exzellenter Sprachkommunikationslösungen zurück und zählt damit zu den global führenden Unified Communications-Anbietern. Wir verfügen über Niederlassungen in über 100 Ländern und bieten umfassende Kommunikations- und Zusammenarbeitslösungen für Unternehmen jeglicher Größe an.

Offene Standards

Open Communications Architecture bedeutet, dass unsere Produkte vollständig auf offenen Standards basieren. Unser Engagement in Sachen offene Standards ist anerkanntermaßen unübertroffen in der Branche. Unsere Kunden profitieren somit von dem Wissen, branchenführende Technologien integriert zu haben, die unser eigenes Portfolio ergänzen. Sie sind somit vor starren Technologielösungen geschützt und können von den Erfahrungen anderer Kunden lernen, die ähnliche Lösungen nutzen. Softwarebasierte Sprach-, Unified Communications- und Contact Center-Lösungen sowie unsere Enterasys Networks-Infrastruktur sind die technologischen Eckpfeiler unseres Portfolios, die durch unser globales Servicenetz und die Möglichkeit einer Lieferung in der gesamten „Cloud“ ergänzt werden. Unsere Kunden genießen somit maximale Flexibilität bei der Wahl, wie Sie zu IP-basierter Unified Communications migrieren möchten. Wir nennen diesen flexiblen Migrationsansatz OpenPath. Jede Kundensituation ist einzigartig und OpenPath versetzt uns in die Lage, genau die richtige Kombination aus Technologie, Service und Finanzierung für die konkreten Anforderungen jedes einzelnen Kunden zu implementieren, während gleichzeitig die mit neuen Technologien verbundenen Risiken und die Kosten minimiert werden.

Vertrauen, Zuverlässigkeit und Innovation

Der Name Siemens steht für Vertrauen, Zuverlässigkeit und Innovation. Unsere Open Communications Architecture, unsere OpenPath-Methodik und das Engagement des gesamten Unternehmens sind darauf ausgerichtet, diese Werte für jeden Kunden zum Leben zu erwecken. Schließlich ist eine zuverlässige, vertrauenswürdige Kommunikation das Fundament eines jeden erfolgreichen Unternehmens.

Weitere Informationen finden sich unter www.siemens-entersprise.com/de bzw. www.enterasys.com.

31

ANSPRECHPARTNER

Autor:
Nicole Dufft
Senior Vice President
+49 (0) 30-28 52 96-0
n.dufft@pac-online.com

Herausgeber:
Pierre Audoin Consultants (PAC) GmbH
Holzstraße 26
80469 München
Tel: +49 (0) 89 232 368-0
Fax: +49 (0) 89 719 62-65
E-Mail: info-germany@pac-online.com

ÜBER PIERRE AUDOIN CONSULTANTS

PAC liefert fokussierte und objektive Antworten auf die Wachstumsherausforderungen der Akteure im Markt für Informations- und Kommunikationstechnologie (ITK) – von der Strategie bis zur Umsetzung.

Pierre Audoin Consultants wurde 1976 gegründet und ist ein unabhängiges Marktanalyse- und Beratungsunternehmen für den Software- und ITK-Services-Markt. Wir unterstützen ITK-Anbieter mit quantitativen und qualitativen Marktanalysen sowie strategischer und operativer Beratung. CIOs und Finanzinvestoren beraten wir bei der Bewertung von ITK-Anbietern und -Lösungen und begleiten sie bei ihren Investitionsentscheidungen. Öffentliche Organisationen und Verbände bauen auf unsere Analysen und Empfehlungen als Grundlage für die Gestaltung ihrer ITK-Politik.

Weitere Informationen unter www.pac-online.de.

UNSERE STANDORTE

PARIS
Pierre Audoin Consultants (PAC)
92, Avenue de Wagram,
F-75017 Paris, Frankreich
Tel: +33(0) 1 56 56 63 33
Fax: +33(0) 1 48 28 41 06
info-france@pac-online.com

MÜNCHEN
Pierre Audoin Consultants (PAC)
Holzstraße 26,
80469 München, Deutschland
Tel: +49(0) 89 23 23 68 0
Fax: +49(0) 89 719 62 65
info-germany@pac-online.com

BERLIN
Pierre Audoin Consultants (PAC)
Am Kupfergraben 6A,
10117 Berlin, Deutschland
Tel: +49(0) 30 28 52 96 0
Fax: +49(0) 30 28 52 96 29
info-germany@pac-online.com

LONDON
Pierre Audoin Consultants (PAC)
2nd Floor
15 Bowling Green Lane
London EC1R 0BD, Großbritannien
Tel.: +44 (0) 207 251 2810
Fax: +44 (0) 207 490 7335
info-uk@pac-online.com

BUKAREST
Pierre Audoin Consultants (PAC)
Louis Pasteur 40
050536 Bukarest - 5,
Rumänien
Tel.: +40 (0) 21 410 75 80
Fax: +40 (0) 21 410 75 81
info-romania@pac-online.com

NEW YORK
Pierre Audoin Consultants (PAC)
192 Lexington Avenue, Suite 1101
New York, NY 10016, USA
Tel: +1(646) 277-7250
Fax: +1(212) 532-0257
info-us@pac-online.com

SAO PAULO
Pierre Audoin Consultants (PAC)
Rua Pedro de Toledo, 130, Office 61
Vila Clementino,
Sao Paulo, 04039-030 Brasilien
Tel.: +55 (11) 5539 0280
Fax: +55 (11) 5539 0280
info-latam@pac-online.com