

Sicher kommunizieren über die Unternehmensgrenzen hinaus

Unified Communications (UC) boomt. Allerdings beäugen viele Manager das Zusammenwachsen von Daten, Sprache und den zugehörigen Anwendungen weiterhin kritisch. Vor allem Federations werfen traditionelle Sicherheitskonzepte über den Haufen und lösen neue Sicherheitsbedenken aus.



Autor:
Marcel Oberli ist als Security Consultant für CASSARIUS tätig. www.cassarius.ch

Durch den Einsatz von Unified Communication öffnet ein Unternehmen seine Infrastruktur und vernetzt sich über die Unternehmensgrenzen hinaus. Der Theorie nach erhöht das die Anfälligkeit gegenüber Angriffen. Obwohl die Installation und Konfiguration von Unified Communications-Lösungen wie Microsofts Office Communications Server (OCS) dank ausgereifter Verschlüsselungstechnologie ausreichend sicher gestaltet werden können, hemmen technische Sicherheitsbedenken weiterhin den Einzug von UC in Unternehmen.

Eine Hemmschwelle bilden Federations.

Mit einer Federation ist die Verbindung von zwei oder mehreren autonomen Unified Communications-Systemen gemeint, über welche komplett voneinander getrennte Unternehmen ihre Geschäftsprozesse grenzüberschreitend abwickeln können. Den Federation-Partnern steht dabei die gesamte UC-Funktionalität wie Präsenzinformationen und Instant Messaging zur Verfügung.

Bleiben wir beim Beispiel Microsoft: Federations kommunizieren verschlüsselt (mutual TLS) über Internet. Zur Einrichtung einer Federation sind keine manuellen Handlungen von ICT-Spezialisten gefragt. Jeder Mitarbeitende kann die Verbindung automatisch herstellen, indem er die gesuchte, firmenexterne Kontaktperson seinem Office Communicator hinzufügt. Die gewünschte Federation wird im Hintergrund automatisch aufgebaut und los geht's. Die zwei Parteien

können sofort mit einander kommunizieren.

Diese Art unternehmensüberschreitender Vernetzung birgt jedoch gewisse Sicherheitsrisiken. Wenn ein Angreifer einen eigenen Office Communications Server installiert, kann er mittels Brute Force Attacke versuchen, Mitarbeitende des ausgesuchten Opferunternehmens zu seinem Office Communicator Client hinzuzufügen. Ist er in der Lage einen Benutzer erfolgreich hinzuzufügen, bestätigt sich, dass dieser auch wirklich existiert.

Diese Methode verhilft dem Angreifer in der Regel zu vielen gültigen E-Mailadressen, weil die Benutzer innerhalb einer Unified Communications-Infrastruktur meistens über ihre E-Mailadresse identifiziert werden. Hinzu kommt die Tatsache, dass E-Mailadressen häufig auch für die ActiveDirectory-Anmeldung eingesetzt werden. Nutzt der Angreifer die Sicherheitsanfälligkeit erfolgreich aus, könnte er beispielsweise auf Outlook Web Access des Opferunternehmens zugreifen oder gar, mittels Remote Access, ins interne Firmennetzwerk gelangen.

Microsoft hat diese Gefahr erkannt und dem Office Communications Server (OCS) zwei Sicherheitsmechanismen eingebaut.

Einerseits erlaubt der OCS nur eine gewisse Anzahl Anfragen für verschiedene Benutzernamen in einer bestimmten Zeitspanne. Überschreitet ein fremder OCS diese Anzahl,

werden sämtliche weiteren Zugriffsversuche gesperrt. Auf diese Weise wird verhindert, dass Brute Force Attacken mit sehr vielen verschiedenen Anfragen in sehr kurzer Zeit erfolgreich sind.

Andererseits gewährt ein Office Communications Server einem fremden OCS zu Beginn nur ein sehr begrenztes Datenvolumen. Ein fremder OCS, der zum ersten Mal eine Verbindung zum Zielsystem aufbaut, wird nur sehr wenige Daten übertragen können. Der Zielsystem untersucht diese Daten sofort. Ist die Anzahl gültiger Zugriffsversuche des fremden OCS sehr hoch, wird entsprechend mehr Datenvolumen zugelassen. Werden jedoch sehr viele ungültige Zugriffsversuche erkannt, wie es bei einer Brute Force Attacke der Fall wäre, wird das erlaubte Datenvolumen umgehend stark reduziert. Eine Brute Force Attacke würde somit sehr lange dauern.

Um legitime hohe Datenvolumen mit befreundeten Unternehmen nicht unnötig einzuschränken, hat der Administrator die Möglichkeit, Geschäftspartner auf eine sogenannte weisse Liste (white list) zu setzen. Für alle Office Communications Server in dieser «white list» entfallen die beiden oben beschriebenen Restriktionen komplett. Es existiert zudem eine «black list», in welche unerwünschten Kommunikationspartner aufgenommen werden können.

Ist es generell nicht erwünscht, dass Federations von intern oder von extern aufgebaut werden können, besteht die Möglichkeit diese Funktion einzuschränken oder ganz zu deaktivieren.

Federations sind nur ein Sicherheitsaspekt unter vielen, welche beim Einsatz von Unified Communications berücksichtigt werden müssen.