

Siemens Enterprise Communications

München, 21. Oktober 2008

OpenScale Security Services erhöhen die Sicherheit von Unified Communications

Neue Professional Services und Lösungen unterstützen und sichern Unified Communications-Umgebungen

Siemens Enterprise Communications erweitert sein Angebot an OpenScale-Services um Elemente und Funktionen, die die Sicherheit von Unified-Communications-Lösungen in Unternehmen wesentlich verbessern. Das neue Portfolio reicht von Professional und Managed Services über spezielle Wartungsleistungen bis hin zu Benutzerschulungen. Diese so genannten OpenScale Security Services zielen auf Unternehmen, die Unified-Communications-Anwendungen und -Infrastrukturen betreiben, insbesondere in heterogenen Umgebungen. Mit den OpenScale Security Services deckt Siemens vier Kernbereiche ab: Business Continuity, Compliance, Identity & Privacy und Threat Mitigation & Data Security.

CIOs befassen sich zunehmend mit dem Thema Sicherheit von Unified Communications (UC). Eine Sensibilisierung für mögliche Risiken bei der Nutzung neuartiger Kommunikationsmittel entsteht unter Umständen sogar bereits vor der Einführung von UC durch schlechte Erfahrungen etwa mit Grey-Net-Attacken. Das sind Schadprogramme, die über Instant-Messaging- oder Peer-to-Peer-Anwendungen, welche Mitarbeiter ohne das Wissen der IT-Abteilung herunter geladen haben, angreifen. Zu den Sicherheitsrisiken von UC zählen das Abhören von Voice-over-IP-Gesprächen, das Ausspähen von Instant Messages und anderem Datenverkehr, gefälschte Anruferkennungen oder Instant-Messaging-Identitäten sowie DoS (Denial of Service)-Angriffe auf die Kommunikationsinfrastruktur. Die OpenScale Security Services von Siemens Enterprise Communications können Unternehmen bei der Abwehr dieser Gefahren helfen.

"Wenn Kunden von Unified Communications uneingeschränkt profitieren sollen, ist es unerlässlich, neue Service-Angebote zur Verfügung zu stellen und Sicherheitsprobleme bereits im Vorfeld zu klären. Unified Communications wirkt sich auf sämtliche Prozessebenen aus - von der Infrastruktur

bis zur Integration in Geschäftsabläufe - und birgt damit ein großes Gefahrenpotenzial für die Sicherheit", erklärte Wolfram Funk, Senior Advisor bei der Experion Group.

Das neue Sicherheits-Dienstleistungsportfolio baut auf dem bestehenden OpenScale-Services-Angebot für UC-Anwender auf. Damit können Unternehmen – unabhängig von ihrer Größe, geografischen Aufstellung oder ihrer Ausstattung mit eigenem Fachpersonal und vorhandenen Systemen – Unified-Communications-Dienste beziehen. Die neuen OpenScale Security Services schließen sowohl Siemens-eigene UC-Lösungen als auch Infrastrukturelemente, Kommunikationssysteme und -anwendungen sowie Endgeräte von Drittanbietern ein. Diese Dienste helfen Unternehmen, die eine UC-Lösung implementieren, Sicherheitslücken frühzeitig zu erkennen und effektive Maßnahmen zur Risikominimierung umzusetzen. Darüber hinaus ermöglichen sie eine laufende Überwachung für den ständigen Schutz von Daten und Ressourcen.

Die UC-Lösungen von Siemens Enterprise Communications wie OpenScape UC Server, OpenScape Voice und ähnliche Produkte enthalten bereits Security-Funktionen. Die starke Verzahnung mit Office-Anwendungen, Programmen für die Zusammenarbeit (Collaboration) oder mit betriebswirtschaftlicher Software erhöht allerdings die Komplexität und das Gefahrenpotenzial. Durch die Zusammenführung von der Festnetz- und Mobilkommunikation mittels Fixed-Mobile-Convergence-Lösungen wird diese Problematik noch verstärkt. Mit den neuen OpenScale Security Services unterstützt Siemens die Anwender seiner UC-Lösungen durch Leistungen wie Evaluierung, Beratung, Implementierung, Wartung und Schulung sowie die Einbettung in ein Sicherheits-Gesamtkonzept. Dank ihrer Offenheit lassen sich die OpenScale Security Services auch auf heterogene Infrastrukturen mit Produkten verschiedener Hersteller anwenden. Siemens-Kunden können alle nötigen Dienstleistungen aus einer Hand beziehen und vom Know-how von über 350 Sicherheitsexperten profitieren. Diese kümmern sich um die Einhaltung unternehmensweit einheitlicher Richtlinien und Prozesse.

„Unternehmen interessieren sich zwar lebhaft für die zahlreichen Vorteile von Unified Communications, aber viele haben auch Bedenken wegen der Sicherheitsrisiken“, erklärte Marc Kleff, Vice President Professional Services and Solution Management – Security bei Siemens Enterprise Communications. „Wir haben auf der Basis unserer Erfahrungen mit offenen Unified Communications ein umfassendes Portfolio von Security-Dienstleistungen für die wesentlichen Problemfelder entwickelt, sodass sich CIOs darauf verlassen können, dass ihre Kommunikationsinfrastruktur so sicher wie möglich ist.“

Die neuen OpenScale Security Services decken vier Kernbereiche ab: Business Continuity, IT-

Compliance, Identity & Privacy und Threat Mitigation & Data Security. Die entsprechenden Services helfen Unternehmen, die eine UC-Lösung implementieren, Sicherheitslücken in einem frühen Stadium festzustellen, effektive Maßnahmen zur Bekämpfung von Schwachstellen umzusetzen und durch fortlaufende Überwachung sicherzustellen, dass ihre Daten und ihr Betriebsvermögen zu jedem Zeitpunkt geschützt sind.

Business Continuity

Schwerpunkt des Business-Continuity-Managements sind Strategien, die sicherstellen, dass ein Unternehmen die Schlüsselkomponenten seiner UC-Umgebung bei einem Systemausfall oder einem Notfall wiederherstellen kann. Die Business-Continuity-Services von Siemens Enterprise Communications helfen Abläufe festzulegen und Pläne zu erstellen, mit denen alle Probleme erfasst werden können und Unternehmen in der Lage sind, eine ständig verfügbare, katastrophensichere Kommunikationsumgebung bereitzustellen.

IT-Compliance

Die Dienstleistungen rund um IT-Compliance beinhalten Audits, so genannte Health Checks und die Festlegung von Firmen-Richtlinien (so genannten Policies). Mit diesen Maßnahmen kann ein Unternehmen gewährleisten, dass seine Security- und Continuity-Vorkehrungen die Corporate-Governance-Ziele und die gesetzlichen Vorgaben erfüllen. Dazu zählen etwa eine Instant Messaging Policy sowie Kontroll- und Nachverfolgungsmöglichkeiten für UC-Umgebungen. Siemens Enterprise Communications erarbeitet zusammen mit dem Unternehmen ein flexibles, umfassendes Regelwerk zur Informationssicherheit, das Risiken minimiert, ohne die Agilität zu beeinträchtigen.

Identity & Privacy

UC-Umgebungen können auch Bedenken in Hinblick auf Sicherung der Identität von Einzelpersonen auslösen. Benutzer müssen sich darauf verlassen können, dass sie wirklich mit dem gewünschten Gegenüber kommunizieren. Angreifer könnten gefälschte Anruferkennungen oder Instant-Messaging-Identitäten nutzen um vorzutäuschen, sie würden Mitarbeiter beispielsweise als IT-Administrator kontaktieren, um vertrauliche Informationen wie Passwörter zu erschleichen, mit denen sie weitere Attacks starten oder Informationen ausspionieren können. Die Identity- und Privacy-Services von Siemens Enterprise Communications stellen Geschäftsprozesse, Richtlinien und Technologien bereit, mit denen die Unternehmen den Zugriff der Benutzer auf kritische Online-Anwendungen und Ressourcen verwalten und steuern können. Gleichzeitig sorgen sie für den kostengünstigen Schutz vertraulicher personen- und unternehmensbezogener Informationen gegen den Zugriff durch unautorisierte Benutzer.

Threat Mitigation & Data Security

Die Threat-Mitigation- und Data-Security-Services umfassen sicheres Design, Implementierung und Tests der in UC-Umgebungen typischerweise stark heterogenen Infrastrukturkomponenten und Anwendungen. Dazu zählen beispielsweise Firewalls, VPNs, Intrusion-Detection-Systeme und allgemeine Netzwerk-Security-Komponenten, um Angriffe abzuwehren. Beispielsweise können Telefone oder Softphones so manipuliert werden, dass sich deren Mikrofone ohne Abheben des Hörers aktivieren lassen. Dadurch könnten beispielsweise persönliche Gespräche aus der Ferne belauscht werden. Mit einer DoS-Attacke, die bei der traditionellen Telefonie praktisch unbekannt war, können die heutigen Angreifer die Kommunikationsinfrastruktur stören, indem sie Telefone oder Netzwerke überlasten bzw. vollkommen lahm legen. Die Folge ist, dass das Unternehmen nicht mehr per E-Mail oder Telefon kommunizieren kann und praktisch von der Außenwelt abgeschnitten ist. Siemens Enterprise Communications bietet Datenverschlüsselungs-Services und VPN-Lösungen, die ein Abhören der Kommunikation unmöglich machen. Ebenso stellt das Unternehmen so genannte Perimeter-Security- und Content-Security-Lösungen bereit, die gegen Gefahren schützen, die mit Echtzeit-Anwendungen einhergehen.

Siemens Enterprise Communications ist ein Joint Venture zwischen The Gores Group, einem führenden Finanzinvestor mit Sitz in den Vereinigten Staaten, und der Siemens AG. In das Joint Venture gehen die Siemens Enterprise Communications GmbH & Co. KG, ihre weltweiten Verbundunternehmen sowie Enterasys Networks und SER Solutions ein. So entsteht ein neuer Marktführer im Bereich Enterprise Communications mit besonderen Stärken bei Unified Communications, Contact Centers und sicheren Netzwerken. Über 14.000 Mitarbeiter weltweit bieten mit dem Open Communications-Ansatz Enterprise Communications- und Netzwerklösungen für Unternehmen jeder Größe. Geschäftsprozesse werden damit produktiver, schneller und sicherer. Und dies unabhängig von der Netz- oder IT-Infrastruktur. Im Geschäftsjahr 2007 erzielte Siemens Enterprise Communications einen Umsatz von etwa 3,2 Milliarden Euro. Weitere Informationen zu Siemens Enterprise Communications finden Sie unter www.siemens.com/open.

Siemens Enterprise Communications GmbH & Co. KG is a Trademark Licensee of Siemens AG.