

Die Geschäftswelt verändert sich...

...und was ist mit Ihrer Sicherheit?

Siemens Enterprise Communications

2011

1. Zusammenfassung

Die Geschäftswelt verändert sich...

Derzeit findet ein Paradigmenwechsel bei sozialen und technologischen Trends statt, der die Kommunikationslandschaft in Unternehmen grundlegend verändern wird.

Die zunehmende „Consumerization“, die soziale Vernetzung und die Mobilität sowie Weiterentwicklungen im Bereich der Sicherheit und der flexiblen Bereitstellungsmodelle werden die Art, wie Unternehmen auf Informationen zugreifen, wie sie zusammen arbeiten und wie sie Beziehungen mit Kunden aufbauen dauerhaft verändern.

Wir bezeichnen diese Entwicklung als „Kommunikationsrevolution“: Eine Trendwende, die für Unternehmen das neue Zeitalter der Cloud Communications einläutet.

Die Cloud überzeugt

Die Vorteile der Cloud liegen klar auf der Hand: Unternehmen müssen weniger Vorabkosten einrechnen, benötigen weniger technisches Fachwissen und können ihre Geschäftsvorgänge insgesamt vereinfachen. Darüber hinaus können Unternehmen ihre Geschäfte schnell und einfach nach oben und unten skalieren, virtuelle Organisationen schaffen, ohne geografische Grenzen oder physische Rechenzentren berücksichtigen zu müssen. Außerdem können sie alle für die Kommunikation und Zusammenarbeit notwendigen Dienste bereitstellen.

Durch die Befreiung von kabelgebundener Kommunikation profitieren sowohl große als auch kleine Unternehmen von neuen und leistungsstarken Kommunikationsmöglichkeiten.

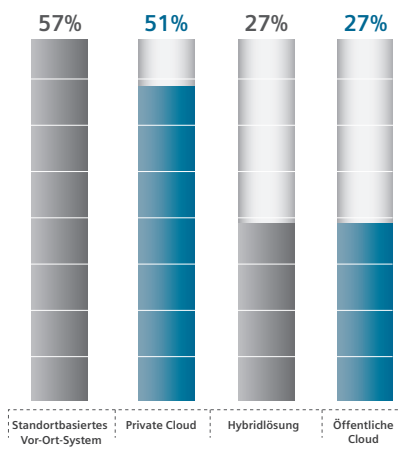
Letztendlich bedeutet dies, dass die Mitarbeiter von beinahe jedem Gerät und Standort eine Verbindung zu der Kommunikationsanwendung ihrer Wahl herstellen können, sei es ein Sprachdienst, eine Webkonferenz oder Instant Messaging. Darüber hinaus macht das Internet die Zusammenarbeit mehrerer Mitarbeiter innerhalb des Unternehmens und über das Unternehmen hinaus zu einem Kinderspiel.

Einfach gesagt: Durch die Cloud verfügen Unternehmen über effizientere Kommunikationsmöglichkeiten, bessere und kontrolliertere Zugriffsmöglichkeiten sowie eine beeindruckende Flexibilität, Mobilität und Skalierbarkeit.

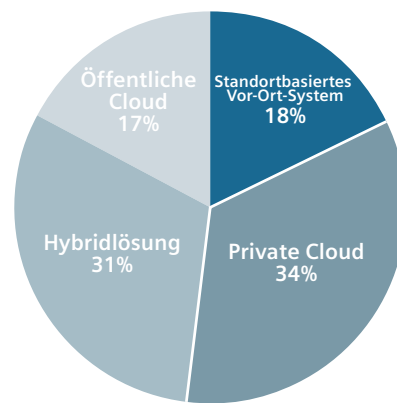
Eine neue Perspektive

In der Tat erwarten CIOs als Resultat aus dieser Entwicklung, dass die Modelle mit privater Cloud oder Hybridlösungen in den kommenden zwei Jahren die Modelle reiner standortbasierter Vor-Ort-Lösungen an Bedeutung überholt haben werden.

Heutzutage dominieren hauptsächlich standortbasierte Modelle¹



In zwei Jahren werden Cloud- und Hybridmodelle dominieren¹



Aber in dieser stark vernetzten neuen Welt müssen wir uns einer neuen Herausforderung stellen: der Sicherheit. Und zuallererst müssen Sie eine ehrliche Antwort auf die Frage finden: Ist Ihr Unternehmen wirklich oder nur scheinbar sicher?

1. Loudhouse Research, September, 2011.

2. Sicherheitsanforderungen verändern sich

Sind Sie vor Bedrohungen geschützt?

Soziale Medien haben uns im Sturm erobert und uns die Möglichkeiten unbegrenzter Mobilität und flexibler Nutzung und Bereitstellung eröffnet. Wir können nun frei wählen, wie, wann und wo wir mit wem kommunizieren. Die Kommunikationsrevolution hat eine grundlegende Veränderung in der Art und Weise, wie Unternehmen heutzutage Geschäfte betreiben, ausgelöst.

Für ein Unternehmen bedeutet diese Veränderung, sich auch Gedanken über die potenziellen Sicherheitsrisiken zu machen, die diese Revolution mit sich bringt.

Denn neben allen Vorteilen – unbegrenzte Mobilität, soziale Zusammenarbeit, intelligente Geräte mit sofortigem Zugriff auf beliebige Anwendungen oder Datenquellen – birgt die offene Struktur unserer vernetzten Welt auch Gefahren.

Wie im „No Jitter Blog for Connected Enterprises“ einmal so treffend festgestellt wurde: „Die unbequeme Wahrheit ist: Je mehr wir kommunizieren – über Sprache, IM, SMS, E-Mails, Videos –, desto größer wird die Angriffsfläche für potenzielle Attacken. Und je mehr dieser Datenverkehr über drahtlose Geräte und Netzwerke zunimmt, desto angreifbarer machen sich Unternehmen.“

Der explosionsartige Anstieg von unstrukturierten Daten (79 %), Mobilität (63 %) und der Nutzung von Web 2.0 (52 %) allein von 2009 bis 2010 sollte Grund genug sein, die wachsende Bedrohung ernst zu nehmen. Und wir dürfen nicht die Augen davor verschließen, dass dies erst der Anfang ist.

Wie hoch ist das Risiko?

In unserer heutigen vernetzten Welt sind Cyber-Attacken nicht mehr nur Science-Fiction, sondern längst Realität. Allein in diesem Jahr haben 29 % aller Unternehmen eine Zunahme von Angriffen gemeldet, und 79 % aller Unternehmen waren in den letzten 12 Monaten Opfer einer solchen Cyber-Attacke.

Wie hoch sind die Kosten?

7,2 Mio. US-Dollar kostet Unternehmen durchschnittlich eine Sicherheitslücke.

Im Jahre 2010 erbeutete eine einzige rumänische Hackerbande in nur wenigen Monaten 15,8 Mio. US-Dollar.

2.200 Unternehmen in den USA wurden von einem einzigen Hackerteam angegriffen.

Hacker werden immer gerissener und mutiger, und wenn Sie genauer hinsehen, werden Sie erkennen, dass vernetzte Unternehmen immer angreifbarer werden.

Je mobiler Unternehmen bzw. ihre Mitarbeiter sind, desto höher ist die Zahl der potenziellen Schwachstellen. Dies bedeutet wiederum: Je mehr Daten im Unternehmensnetzwerk gespeichert werden, desto höher ist das Risiko, dass diese gestohlen werden können.

Dies liegt vor allem an netzwerkübergreifenden Zugriffen, der Vielzahl an Zugriffspunkten und der Anzahl an externen Teilnehmern (mobile Mitarbeiter und Mitarbeiter im Home Office, Partner, Lieferanten und Kunden).

Die wachsende Nutzung von Mitarbeiter eigenen sog. „intelligenten“ Geräten wie Smartphones für arbeitsbezogene Tätigkeiten stellt ebenfalls ein ernstes Sicherheitsproblem für CIOs dar. Nicht nur die Aufrechterhaltung zentraler Sicherheitsrichtlinien wird hierdurch erschwert, sondern die steigende Zahl von Attacken auf Smartphones sowie Downloads aus App-Stores durch Mitarbeiter bieten darüber hinaus auch potenziell unbekannte Angriffspunkte für Viren und Schadsoftware.

Die Realität ist, dass die Nutzung von Mobiltelefonen, Laptops, Web 2.0-Anwendungen, Videos und anderen sozialen Medien im Privathaushalt, bei der Arbeit und auf Geschäftsreisen zu immer komplexeren Systemen führt, deren Schutz immer schwieriger wird.

Sicherheits-Mythen und -Tatsachen

Der Kampf um die Unternehmenssicherheit hat sich geändert: Heutzutage geht es nicht mehr nur um den einfachen Datenschutz. Da auch Sprachkommunikation und Unified Communications-Anwendungen IP-basiert sind und außerhalb der eigenen Firewall agieren, sind sie ebenfalls anfällig für Cyber-Attacken.

Eine wachsende Bedrohung

- 50 % mehr Attacken auf VoIP und UC zwischen 2009 und 2010
- 25 % aller Hackerangriffe zielen auf Voice- und UC-Anwendungen
- In Spitzenzeiten findet alle 2 1/2 Minuten ein Angriff auf VoIP- und UC-Anwendungen statt

Da VoIP- und UC-Systeme mit externen Netzwerken und direkten Voice-to-Voice-Services zusammenarbeiten, eröffnen Unternehmen Angreifern neue Möglichkeiten zu Attacken auf zugrunde liegende Netzwerkkomponenten. Und all das bedeutet für Ihr Unternehmen ein höheres Risiko.

Durch sogenannte „Lauschangriffe“ (Eavesdropping) können Hacker Namen, Kennwörter und Telefonnummern ausspähen und so die Kontrolle über Voicemail, Telefentarife, Anrufweiterleitungen und Rechnungsinformationen oder Zugriff auf Geschäftsdaten erhalten. Und genau wie Computer sind auch VoIP-Softphones für Würmer, Viren und Schadsoftware angreifbar. Sogenannte „Denial-of-Service“-Attacken können Sprachservices lahmlegen oder bieten einen Schutzschild für Angreifer, um Anrufe weiterzuleiten oder zu hacken.

Die Bewertung der potenziellen Risiken für das gesamte Unternehmen ist ein wichtiger erster Schritt. Eine Übersicht über die Schwachstellen im System zu erhalten, ist jedoch oftmals eine Herausforderung. Das liegt unter anderem an den sich ständig verändernden Sicherheitsbedingungen.

Aufgrund der wirtschaftlichen und geopolitischen Lage ist heutzutage jedes Unternehmen ein potenzielles Ziel für Cyber-Kriminalität und Cyber-Terrorismus. Die primären externen Bedrohungen und Risiken – Gebührenbetrug, Lauschangriffe, Phishing, Vishing (ID-Attacken auf VoIP-Datenverkehr) und SPIT – sind üblicherweise finanziell motiviert. Vernachlässigen Sie jedoch nicht mögliche interne Sabotageakte. Für Unternehmen bedeutet dies, noch einmal darüber nachzudenken, was Sicherheit tatsächlich bedeutet. Wenn Sie die Vertraulichkeit, Integrität und Verfügbarkeit Ihres Unternehmens sicherstellen möchten, müssen Sie Sicherheit zu einem integralen Bestandteil aller Geschäftsabläufe machen. Sicherheit - von Anfang an!

Das Risikoprofil von Webkonferenzen

Webkonferenzen erlauben jedem, der über eine Internet-Verbindung verfügt, die Zusammenarbeit mit anderen Personen: Chatten, Konzepte und Ideen erörtern, Bildschirme freigeben, Dateien übermitteln und auf virtuelle Whiteboards zugreifen. Doch indem Sie persönliche Besprechungen durch Webkonferenzen ersetzen, werden möglicherweise wichtige Informationen für Personen außerhalb des Unternehmens sichtbar.

- Wenn ein Webkonferenzserver infiltriert wird, sind die Daten möglicherweise für andere sichtbar, die Zugriff auf diese Umgebung haben.

- Wenn Endbenutzersysteme (Betriebssysteme oder Webbrowser) oder die Client-Software für Webkonferenzen auf den Geräten der Teilnehmer von Spyware oder von ferngesteuerten Botnet-Programmen manipuliert werden, werden möglicherweise sensible Daten für andere zugänglich.
- Nicht autorisierte Teilnehmer erhalten möglicherweise Zugriff auf Inhalte, die nicht für sie bestimmt sind, während andere Teilnehmer das Risiko möglicherweise noch gar nicht erkannt haben.
- Passive Teilnehmer einer Webkonferenz könnten versehentlich nicht für die Öffentlichkeit bestimmte Inhalte über Instant Messaging- oder Audio-Funktion weitergeben.
- Ignorieren Sie beispielsweise cloudbasierte File Sharing Dienste innerhalb einer gesicherten Web-Konferenz, tragen Sie so indirekt zu einem erhöhten Risiko bei, dass nicht berechtigte Personen Zugriff auf diese Inhalte bekommen.

3. Sicherheit von Anfang an

Neue Attacken, die durch die Nutzung von Cloud Computing, Mobilität, sozialer Medien und durch unzureichende IT-Sicherheit begünstigt werden, bedeuten für ein Unternehmen, dass es neue Strategien für sein IT-Sicherheitskonzept entwickeln muss.

Die wichtigsten Bereiche für Sicherheit sind immer noch die Authentifizierung, die Identität und das Auditing. Wenn es jedoch um Ihre Unternehmenskommunikation (und damit Ihre Daten) geht, sollten Sie Sicherheit als grundlegenden Aspekt Ihrer Voice- und UC-Anwendungen betrachten, ungeachtet dessen, ob Sie Ihre Cloud privat, öffentlich oder als Hybridmodell bereitstellen.

Kann ich also der Cloud vertrauen?

Das hängt davon ab, ob Sie unsere OpenScape Secure Cloud Services verwenden.

Falls ja, können Sie Ihrer Cloud problemlos vertrauen, da OpenScape Secure Cloud eine für Unternehmen notwendige sichere und stabile Kommunikationsinfrastruktur mit standardmäßig integrierter Notfallwiederherstellung bietet.

Jeder Sicherheitsaspekt wird berücksichtigt – von der integrierten Ausfallsicherheit bis zur Anwendung



von Best Practices und Standards, die die Integrität Ihrer Kommunikation und Daten zwischen Gerät und Netzwerk oder Rechenzentrum sicherstellen.

Unsere Services werden in redundanten und geografisch verteilten Rechenzentren — die höchsten Anforderungen entsprechen — gehostet, die von einem unabhängigen Institut mit dem höchsten Branchenstandard (Tier 4 TIA-942) ausgezeichnet wurden. Darüber hinaus wird das OpenScape Secure Cloud Services-Netzwerk rund um die Uhr überwacht, verwaltet und kontrolliert.

Des Weiteren werden verschiedene Sicherheitsmechanismen wie Firewalls und Session Border Controller eingesetzt, um die Rechenzentren gegen Virus-Attacken zu schützen. Die Verschlüsselung von Voice-Signalen und Payload verhindert Lauschangriffe auf Telefonanrufe. Wir führen darüber hinaus regelmäßige Penetrationstests für alle unsere Services durch, damit Sie jederzeit einen vollständigen Schutz genießen.

Integrierte Sicherheitsfunktionen

Bei Siemens Enterprise Communications nehmen wir Sicherheit sehr ernst. Darum haben wir unser Cloudnetzwerk sowie unsere Voice- und Datenprodukte, Lösungen und Services mit umfangreichen Sicherheits- und Zuverlässigkeitsfunktionen ausgestattet, die nichts dem Zufall überlassen.

Als Experte im Bereich IT Sicherheit werden Sie bemerken, dass wir alle grundlegenden Aspekte abdecken: Von Identitätsmanagement und Anwender-Provisionierung bis zur Sicherung von Inhalten und Kontrollen für Authentifizierung und Netzwerkzugriff, mit denen unberechtigte Zugriffe aus nicht vertrauenswürdigen Netzwerken verhindert werden. In jeder Phase des Prozesses (vom ersten Codieren bis zum Penetrationstest) werden alle unsere Services unter dem Aspekt der Sicherheit entwickelt.

Sicherheits-Fakten

Unsere integrierten Ende-zu-Ende Sicherheitsfunktionen decken alle Bereiche ab: Vom Schutz der Zugriffspunkte für Endbenutzer bis zur verschlüsselten Speicherung und Übertragung von Daten sorgen unsere besten Sicherheitslösungen dafür, dass stets alle Anforderungen einer sich verändernden Welt der Bedrohungen erfüllt werden.

Darüber hinaus steht Ihnen unser Professional und Managed Services-Team jederzeit für Implementierungs- oder Wartungsaufgaben zur Verfügung, sodass Ihre Cloud Communications-Anwendung jederzeit verfügbar und geschützt ist.

Der Ansatz von Siemens Enterprise Communications

Zusammen mit unserem Partner Enterasys, einem Unternehmen der Siemens Enterprise Communications-Gruppe, bieten wir das umfangreichste Portfolio an Sicherheitsanwendungen in der gesamten Branche. So können wir alle Anforderungen, die Sie an Ihr Netzwerk oder Ihre UC und VoIP-Kommunikation stellen, jederzeit erfüllen.

Das ist jedoch noch nicht alles. Wenn es darum geht, den richtigen Personen Zugriff auf Ihre Kommunikationsinfrastruktur zu gewähren, bieten Ihnen unsere Services integrierte Zugriffskontrollen, sodass Sie Ihre UC-Anwendungen an jedem Endpunkt und jedem Standort innerhalb eines Netzwerkes bereitstellen können. So sind Ihre Niederlassungen, Call Center, mobile UC-Anwendungen auf Smartphones und Zusammenarbeitsumgebungen mit Partnern immer auf dem neuesten Stand.

4. Nehmen Sie uns beim Wort

Unsere Cloud-Services mit den preisgekrönten Anwendungen OpenScape UC Suite und OpenScape Voice bieten Ihnen ein umfangreiches Portfolio an Unified Communications and Collaboration-Funktionen über die Cloud. All unsere Services sind mit der sichersten und zuverlässigsten Technologie der Branche ausgestattet.

In über zehn Jahren haben wir umfassende Erfahrungen im Bereich VoIP und UC gesammelt und Hunderte Identitäts- und Sicherheitslösungen implementiert. Unsere Automated Networks waren die ersten, die Sicherheitsfunktionen in Switching und Verwaltung integrierten. Und damit wir unsere Vorstellung der „offenen Cloud“ realisieren konnten, haben wir nachhaltig in die technische Expertise investiert, um herstellerübergreifend unterschiedliche Technologien integrieren zu können.

Durch unser umfangreiches Angebot an drahtgebundenen und drahtlosen Netzwerkinfrastruktur- und Sicherheitslösungen von Enterasys können wir Unternehmen mit unserer einzigartigen Kombination an Automatisierungs-, Sichtbarkeits- und Steuerungsfunktionen dabei unterstützen, ihre IT-Kosten zu senken und gleichzeitig die betriebliche Effizienz und Produktivität zu steigern.



Aufgrund unserer langjährigen Erfahrung in Bereichen mit hohen Sicherheitsanforderungen wie dem öffentlichen Sektor und dem Verteidigungssektor vertrauen Kunden auf der ganzen Welt uns bei der Entwicklung von Sicherheitskonzepten für Ihre Sprach- und Datenservices.

Die Einhaltung aller Sicherheitsstandards, -empfehlungen und -verordnungen von Regierungsbehörden, der European Network and Information Security Agency (ENISA), dem National Institute of Standards and Technology (NIST), der britischen nationalen Behörde für Informationssicherheit (CESG) und dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) hat für uns immer höchste Priorität.

Know-how im Bereich Sicherheit

Sie können sich auf uns verlassen: Durch unsere Position als führendes Unternehmen im Bereich Sicherheit bieten wir Ihnen die professionellen Services an, die Sie benötigen, um Ihre Unternehmensumgebung zu schützen.

Unsere Kompetenzzentren für Identity & Access Management, Security & Networks und unser Security Network Operations Center sind immer auf dem neuesten Wissensstand, um die Sicherheit in Ihrem Unternehmen bewerten zu können, Bedrohungen zu verhindern und um so sicherzustellen, dass Sie jederzeit auf den Schutz Ihrer Echtzeitkommunikation vertrauen können.

Wir sind Experten in Sachen Sicherheit

▪ Sicherheit von VoIP

Mehr als zehn Jahre Erfahrung im Bereich VoIP und UC

▪ Identity and Privacy

Hunderte implementierter Identity and Privacy-Lösungen

▪ Threat Mitigation and data security

Über 15 Jahre Erfahrung in Threat Mitigation and data security

▪ Automated Networks

Enterasys war das erste Unternehmen, das Sicherheitsfunktionen in Switching und Verwaltung integrierte

▪ Hochsicherheitsbereiche

Wir sind Experten für Bereiche mit hohen Sicherheitsanforderungen (öffentlicher/ militärischer Sektor)

▪ Offener Ansatz

Wir verfügen über die Erfahrung und das technische Fachwissen, um Technologien verschiedener Anbieter zu integrieren

▪ Umfangreiche Sicherheitslösungen

Basierend auf den Technologien führender Anbieter von Sicherheitslösungen sowie auf standardbasierten Kommunikationslösungen

5. Nächste Schritte

Bei Siemens Enterprise Communications wissen wir, dass jedes Unternehmen seine eigenen Anforderungen hat. Deshalb sind wir auch der einzige Anbieter mit umfassenden Voice-, UCC- und Contact Center-Lösungen für standortbasierte Vor-Ort-Lösungen, private und öffentliche Cloud-Lösungen oder für Hybrid-Lösungen. Alle Services basieren auf unserer offenen, zukunftsweisenden und softwarebasierten Architektur. So sind wir in der einzigartigen Position, eine vollkommen objektive Empfehlung speziell für Ihr Unternehmen aussprechen zu können.

Wir verstehen die potenziellen Schwachstellen Ihres Unternehmens und Ihre Herausforderungen im Kampf gegen Sicherheitsbedrohungen. Daher sichern wir unter anderem Ihre IT-Infrastruktur mithilfe von flexiblen Sicherheitslösungen und -Services, die über die modernsten Sicherheits- und Compliancefunktionen verfügen.

Sicherheitslösungen von Siemens Enterprise Communications:

1. Bewährte Sicherheitserfahrungen: Unsere OpenSmart Security Best Practices basieren auf bewährten Erfahrungen und übertreffen in unseren Produkten, Services und Lösungen die von Regierungsorganisationen vorgegebenen Standards und Sicherheitsfunktionen.

2. Umfassendes Sicherheits-Portfolio: Siemens Enterprise Communications bietet das in der Branche umfangreichste UC-Sicherheitsportfolio, einschließlich Produkte, Services und Lösungen.

3. Führende Sicherheitslösungen: Mit unserem Security Ecosystem bieten wir erstklassige Sicherheitslösungen führender Anbieter.

4. Weltweiter, herstellerunabhängiger Sicherheitsservice: Unsere OpenScale Security Services umfassen die Integration, die Implementierung und den Betrieb sowie Cloud-Services — ITIL-konform, herstellerunabhängig und weltweit verfügbar.

5. Sichere Cloud-Services: OpenScape Cloud Services bieten eine Ende-zu-Ende-Sicherheit sowie gegen physische Angriffe geschützte und geographisch redundante Support-Center.

Weitere Informationen über unser Angebot an Sicherheitslösungen finden Sie auf:

www.siemens-enterprise.com/security

Siemens Enterprise Communications ist ein führender Anbieter von End-to-End-Kommunikationslösungen für Unternehmen, in denen eine offene, auf Standards basierende Architektur zur Zusammenführung von Kommunikation und Geschäftsanwendungen für eine nahtlose Zusammenarbeit verwendet wird. Dieses preisgekrönte Konzept von „Open Communications“ ermöglicht Unternehmen mithilfe von leicht bereitzustellenden Lösungen, die sich innerhalb vorhandener IT-Umgebungen einsetzen lassen und die betriebliche Effizienz steigern, eine Erhöhung der Produktivität und Senkung der Kosten. Die Verringerung von Risiken und die kosteneffektive Übernahme von Unified Communications stellt die Grundlage unserer OpenPath-Verpflichtung dar.

Dieses Versprechen wird durch unser OpenScale-Serviceportfolio unterstützt, das internationale, verwaltete und Auslagerungsfunktionen umfasst.

Siemens Enterprise Communications ist ein Joint Venture im Besitz von The Gores Group und der Siemens AG. Das Joint Venture umfasst auch Enterasys Networks, ein Unternehmen, das Netzwerkinfrastruktur und Sicherheitssysteme bereitstellt, die eine perfekte Grundlage für gemeinsame Kommunikationslösungen darstellen.

© 2011 Siemens Enterprise Communications GmbH & Co. KG.

Siemens Enterprise Communications GmbH & Co. KG ist ein Markenlizenznehmer der Siemens AG.

Hofmannstr. 51, D-80200 München, 08/2011

Die in dieser Broschüre bereitgestellten Informationen stellen lediglich allgemeine Beschreibungen oder Eigenschaften der Leistung dar, die im Falle einer tatsächlichen Anwendung nicht immer wie beschrieben zutreffen müssen oder die sich infolge der Weiterentwicklung des Produkts ändern können. Eine Verpflichtung zur Bereitstellung bestimmter Eigenschaften wird nur anerkannt, wenn diese in den Vertragsbestimmungen ausdrücklich vereinbart wurden. Verfügbarkeit und technische Daten können ohne Vorankündigung geändert werden. OpenScape, OpenStage und HiPath sind eingetragene Marken der Siemens Enterprise Communications GmbH & Co. KG. Alle anderen Unternehmens-, Marken-, Produkt- und Servicenamen sind Marken bzw. eingetragene Marken ihrer jeweiligen Eigentümer.