

Neue Konzepte nach einer Migration

VoIP – neue Gefahrenpotenziale?



Foto: shutterstock.com

Voice over IP (VoIP), die Verwendung von IP-basierter Infrastruktur zum Transport von Sprache, ist längst den Kinderschuhen entwachsen: Die Erfahrung aus vielen Telefonie-Migrations-Projekten zeigt uns, dass die Entwicklung von VoIP inzwischen ein vergleichbares Niveau erreicht hat wie Internal-Web-Services und noch mit deutlichem Vorsprung vor beispielsweise Smartphones rangiert.

Während letztere im beruflichen Alltag omnipräsent sind, wir blind Blackberry- von Windows-Mobile-Anwendern anhand des Kluges ihrer Posteingangssignale unterscheiden können, hat sich der Wandel im Umfeld der TK-Plattformen erheblich leiser und unbemerkter vollzogen.

Diese Entwicklung ist nicht weiter verwunderlich, während Intranet und Smartphones dem Anwender neue Funktionen, mehr Flexibilität und Mobilität ermöglichen, ändert sich bei VoIP (wenn es funktioniert wie angedacht) zunächst nichts: Hörer abnehmen, Nummer wählen, Sprache geht unten rein und kommt oben raus. Doch so wünschenswert diese Kontinuität in visueller, auditiver und haptischer Wahrnehmung für den Benutzer auch sein mag: sie birgt aus der Perspektive der Sicherheit ein großes Risiko. Schnell übersieht man, dass sich hinter den baugleichen oder sehr ähnlichen Endgeräten und der

gewohnten Bedienung eine komplett andere Technologie verbirgt. Und mit dem fehlenden Bewusstsein für diese andere Technologie geht fast zwangsläufig ein fehlendes Bewusstsein für andere Gefahrenpotenziale einher.

Schleichende Gefahrenpotenziale

Zusätzlich wird dieser schleichende Übergang durch die Produktpolitik der Hersteller begünstigt. Steht im Rahmen eines normalen Nutzungszyklus heute der Austausch einer konventionellen (Legacy) TK-Anlage an, bietet jeder namhafte Hersteller zumindest als Alternative eine Legacy- und VoIP-beherrschende Hybrid-TK-Anlage. Die Möglichkeiten sind reizvoll: Bestehende Endgeräte können beibehalten werden, die notwendigen Zusatzinvestitionen halten sich im Rahmen und trotzdem bieten diese Systeme die

Vorteile moderner VoIP-Technologie bei gleichzeitigem Investitionsschutz durch die Unterstützung vorhandener konventioneller Geräte. Gleicher Hersteller, gleiches Gehäuse, gleiche Endgeräte und sogar eine ähnliche Modellbezeichnung: Zugegeben, wer hier neue Gefahrenpotenziale nicht vermutet, dem kann man zumindest keine grobe Fahrlässigkeit unterstellen.

Verstärkt wird dieses Risiko durch einen organisatorischen Wandel, der sich aktuell in vielen Unternehmen vollzieht: Die Verantwortung für die TK-Infrastruktur wird verlagert weg von eigens darauf spezialisierten Einheiten innerhalb von Haus- oder Leittechnikbereichen hin in die CIO-Bereiche. Der klassische IT-Bereich wird so zum IKT-Bereich (Informations- und Kommunikationstechnik). Was aus Synergie- und Effizienzgründen durchaus Sinn macht, kann durch Know-how-Verlust jedoch das Risi-

ko weiter erhöhen: Häufig wandern vormals für TK-Technik verantwortliche Mitarbeiter nicht mit in die IT-Abteilungen und so sehen sich gut ausgebildete Spezialisten für IP-Infrastruktur, Server- oder Applikationsbetrieb plötzlich mit einer bislang für sie vollkommen fremden Technologie konfrontiert.

Ein Ignorieren von VoIP als Methode für die Übertragung von Sprache löst das Problem allenfalls kurzfristig: Selbst wenn es – wie häufig der Fall – weder besser noch

Verfälschung sowie Gefahren und Störung der Verfügbarkeit. Die Titel beider Gruppen lassen uns an mögliche Lösungsansätze denken, die wir aus der klassischen IT kennen: Verschlüsselung, Authentisierung und Authentifizierung, Appliances zur Verhinderung von Denial-of-Service-Attacken (DoS). Genau in dieser Überlegung, der Adaption bekannter klassischer IT-Sicherheits-Methoden auf die IP-basierten Kommunikationstechniken, liegt der Schlüssel für die Lösung des Problems.

lich sind, weil eine Veränderung auf dem Transportweg nicht ausgeschlossen werden kann.

Fast alle uns aus dem E-Mail-Verkehr bekannten Varianten dieser Gefahr lassen sich mit etwas Phantasie auf VoIP übertragen: Werbeanrufe von automatisierten Systemen, Anrufe mit gefälschter Absendernummer, VoIP-Viren, die auf dem Zielendgerät das Mikrofon aktivieren und Gespräche aus der Umgebung an den Absender übertragen, VoIP-Viren, die vom Zielsystem aus automatisch teure Sonderrufnummern wählen, Denial-of-Service-Attacken (DoS), die Liste ließe sich beliebig fortführen. Sicherlich ist die Anzahl der aktuell tatsächlich technisch umgesetzten Varianten noch begrenzt, doch, wie in allen anderen Fällen auch, erhöhen sich (meist kriminelle) Kreativität und Motivation für eine Umsetzung überproportional mit der Verbreitung der betreffenden Technologie. Ein entscheidender Unterschied zwischen E-Mail und VoIP erschwert die Implementierung von Schutzmaßnahmen zusätzlich: Während E-Mails durchaus für einen überschaubaren Zeitraum in Quarantäne genommen und mit Hilfe von Filtern und ähnlichen Technologien untersucht werden können, ist eine niedrige Latenz und damit ein möglichst schnelles Weitervermitteln von VoIP-Paketen für eine reibungslose Verständigung unabdingbar. Entsprechend schwieriger gestaltet sich die Kontrolle der einzelnen Pakete.



„Die Verantwortung für die TK-Infrastruktur wird verlagert von eigens darauf spezialisierten Einheiten hin in die CIO-Bereiche.“

Gunnar Haderthauer, Lexta GmbH

kostengünstiger wird, selbst wenn neue Möglichkeiten der Technologie für den konkreten Einsatzfall keine Anwendung finden, der Markt entwickelt sich zweifelsohne in diese Richtung und auf absehbare Zeit werden sich Unternehmen zwangsweise mangels Verfügbarkeit von Legacy-TK-Anlagen mit VoIP auseinandersetzen müssen.

Problem Sicherheitsmechanismus

Wie kann man diesen neuen Gefahrenpotenzialen begegnen? Aufgrund der Technologieunterschiede ist eine ausschließliche Weiterentwicklung und Verstärkung der Sicherheitsmechanismen wie wir sie bislang für klassische TK-Anlagen kennen, die Verhinderung eines physikalischen Zugriffs auf Netz und Anlagen beispielsweise, keineswegs ausreichend.

Grundsätzlich lassen sich die Risiken in zwei Gruppen kategorisieren: Gefahren durch Abhören und

Abhören und Verfälschung

Eine entscheidende Lektion, die wir in den vergangenen 15 Jahren während des Siegesfeldzugs der E-Mail gelernt haben sollten: Die weltweite Verbreitung einer Technologie für die Informationsübermittlung, der Einzug in jeden Haushalt und jedes Unternehmen, garantiert keineswegs eine gleichzeitige, nicht mal eine zeitversetzte, ähnlich große Verbreitung einer dafür adaptierten Technologie zur Sicherung gegen das Abhören und Verfälschen der transportierten Inhalte. Trotz eines inzwischen an vielen Stellen vorhandenen Bewusstseins für die Risiken und die tägliche Konfrontation mit deren offensichtlichsten Auswüchsen, Spam und E-Mail-Viren, gibt es weiterhin keine einheitliche Lösung, um dieser Problematik Herr zu werden. Die hilflos wirkende Minimallösung sind zumeist automatisch angehängte Signaturen mit dem Hinweis, dass weder der Absender noch der Inhalt verläss-

Risiken schmälern

Während Unternehmen für die Absicherung der Kommunikation mit externen Adressaten auf neue Entwicklungen und Standards der Hersteller angewiesen sind und eine konkrete Handlungsempfehlung entsprechend schwerfällt, gibt es für die interne Kommunikation bereits eine Lösung, welche nicht nur Risiken schmälert, sondern auch Vorteile birgt: den Einsatz der bereits vorhandenen Sicherheits-



abhörsichere Kommunikation auf einem Niveau, das noch vor einigen Jahren nur Botschaften und anderen Regierungsstellen vorbehalten war.

Störung der Verfügbarkeit

Die Verfügbarkeiten aktueller VoIP-Systeme liegen merklich unterhalb von denen klassischer TK-Anlagen. Zwar finden sich in Datenblättern meist ähnliche Angaben hierzu, doch während VoIP-Anlagen die angegebenen Werte meist in etwa erfüllen, überschreiten klassische Anlagen diese oft erheblich. Durch selten notwendige Aktualisierungen, wenige Änderungen, lange Produktzyklen und eine über Jahrzehnte ausgereifte Technologie sind dort Verfügbarkeiten von 100 Prozent im Jahresmittel keine Seltenheit. Dieser Reifeprozess steht der noch recht jungen VoIP-Technologie noch bevor. Um sicherzustellen, dass Ausfälle nur durch den noch nicht abgeschlossenen Reifeprozess und nicht durch andere Ursachen erzeugt werden, ist eine intensivere

mechanismen für die IP-Netzwerk-Infrastruktur. Obwohl bei der Tunnelung von VoIP-Paketen über VPN häufig ein nicht unerheblicher Overhead entsteht, erkaufte man sich mit diesem erhöhten Bandbreitenbedarf eine enorme Erhöhung der Sicherheit und erschließt gleichzeitig zusätzliche Anwendungsgebiete. Ein kleines VPN-Gateway samt VoIP-Telefon bei einem im Ausland befindlichen Mitarbeiter oder Geschäftspartner ermöglicht abhörsichere Kommunikation, ohne

selbst, die Leitung zum Teilnehmer und das Endgerät. Da der Anlagenanschluss meist durch den Telefon-Provider verantwortet wird, die Teilnehmer-Leitung zumeist nur gegen mechanische Manipulation oder Defekte geschützt werden muss und das Endgerät durch kostengünstige Ersatzbevorratung schnell ausgetauscht werden kann, konzentrieren sich die Bemühungen im Wesentlichen auf die Anlage selbst. Beim Einsatz von VoIP jedoch finden sich aufgrund des geänderten Übertragungsweges zwischen Anlage und Endgerät erheblich höhere Ansprüche an das verwendete IP-Netzwerk. Um eine ausreichende Sprachqualität sicherzustellen, sind niedrige Latenzzeiten und eine hinreichende Bandbreite notwendig. Der SAP-Druckauftrag eines Kollegen aus dem Nachbarbüro kann schnell ein überraschendes Gesprächsende bedeuten, wenn die eingesetzten aktiven Netzwerkkomponenten kein Quality-of-Service (QoS) beherrschen und deshalb dem VoIP-Datenstrom keine Bandbreite reservieren.



„Die weltweite Verbreitung einer Technologie für die Informationsübermittlung garantiert keineswegs eine gleichzeitige, ähnlich große Verbreitung einer dafür adaptierten Technologie zur Sicherung gegen das Abhören und Verfälschen der transportierten Inhalte.“

Gunnar Haderthauer, Lexta GmbH

sich dabei auf die Integrität eines öffentlichen Telefonanbieters verlassen zu müssen. Ein Laptop oder ein Smartphone mit WLAN-Zugang und einer VoIP-Applikation ermöglichen vertrauliche Telefonate auch aus Ländern, in welchen man sonst auf Berichterstattung mit sensiblen Inhalten über das Telefon verzichtet. Auch die Vernetzung zwischen Standorten ermöglicht so eine

Auseinandersetzung mit der Technologie und ihren Schwachstellen unabdingbar.

Die klassische TK-Anlage

Bei der klassischen TK-Anlage gibt es vier Komponenten, die für einen zuverlässigen Betrieb verantwortlich sind: den Anlagenanschluss an das öffentliche Netz, die Anlage

Die klassische TK-Anlage versorgt bei Stromausfall sich und über eigene Teilnehmer-Leitungen angeschlossene Endgeräte aus der anlageninternen, unterbrechungsfreien Stromversorgung (USV). Bei einer VoIP-Anlage müssen hingegen sämtliche aktive Netzwerkkomponenten entsprechend abgesichert sein. Doch selbst eine USV an jedem QoS-Switch ist längst nicht ausreichend:

Zusätzlich müssen diese Switche Power-over-Ethernet (PoE) unterstützen, um angeschlossene Endgeräte durch die Netzwerkleitung mit Energie zu versorgen. Zwar bieten einige Hersteller als Alternative zu PoE kleine Steckernetzteile an, die bei fehlender Energieversorgung durch die aktiven Netzwerkkomponenten das Telefon selbst mit Strom versorgen. Dieser Lösungsansatz versagt jedoch bei Stromausfall, weil die wenigsten Arbeitsplätze über USV-gestützte Steckdosen verfügen, und birgt auch im täglichen Arbeitsleben Risiken, die der IKT-Hotline überflüssige Kopfschmerzen bereiten: Findet die Gebäudereinigungskraft keine freie Steckdose für den Staubsauger, wird gern mal ein Netzteil ausgesteckt – und das Einstecken nach getaner Arbeit vergessen.

Weitere Störungen

Ein weiterer, gern unterschätzter Punkt ist die notwendige Verfügbarkeit bei Störungen anderer Komponenten: Viele unserer Prozesse und Abläufe stützen sich im Fehlerfall auf die Verfügbarkeit von Sprachverbindungen.

Ob Netzwerkstörung, Stromausfall oder Störungen durch Naturgewalten, im Zweifel verlassen wir uns auf die Kommunikation über das Telefon. Ist dies in dieser Situation auch nicht mehr verfügbar, versagt damit auch der letzte Rückfallplan. Die Bewertung solcher Risiken ähnelt der eines Lottogewinns: Eintrittswahrscheinlichkeit sehr gering, doch Folgen mit erheblichen Auswirkungen.

Fazit

In absehbarer Zeit wird es zu VoIP keine Alternative geben. Risiken sind nicht zu unterschätzen, doch auch Chancen und Möglichkeiten durch die neue Technologie sind attraktiv. Um beides zu adressieren, muss sowohl auf Management- als auch auf Produktionsebene das Bewusstsein vorhanden sein, dass VoIP-TK-Anlagen nicht wie klassische Anlagen annähernd betreuungsfrei und autark funktionieren, sondern ein integraler Bestandteil der IKT-Infrastruktur sind und entsprechende Aufwände für Absicherung und Nutzenoptimierung vonnöten sind.

Gunnar Haderthauer