

WHITEPAPER Redundanz: Wie ausfallsicher ist Ihre Kommunikationsinfrastruktur?

■ Deutsch

innovaphone 
PURE IP COMMUNICATIONS



GET IN TOUCH

innovaphone AG
Böblinger Str. 76
71065 Sindelfingen

Tel. +49 7031 73009-0
Fax +49 7031 73009-9

info@innovaphone.com
www.innovaphone.com

„Redundanz“ (von lateinisch redundare, überlaufen, sich reichlich ergießen) ist das zusätzliche Vorhandensein funktional gleicher oder vergleichbarer Ressourcen eines technischen Systems, wenn diese bei einem störungsfreien Betrieb im Normalfall nicht benötigt werden. [...] In der Regel dienen diese zusätzlichen Ressourcen zur Erhöhung der Ausfall-, Funktions- und Betriebssicherheit.“ (Quelle: Wikipedia)

Kommunikation ist eine der wichtigsten Funktionseinheiten in einem Unternehmen. Sie stellt den internen Informationsfluss ebenso sicher wie den Kontakt zu Kunden und Geschäftspartnern. Ein Ausfall der Kommunikation kann somit große Auswirkungen auf die wirtschaftlichen Ergebnisse haben. Selbst wenn nur Teile der Kommunikation wie etwa ein Vermittlungsplatz oder die Integration in das CRM-System nicht mehr funktionieren, können die Auswirkungen auf die Produktivität und die Zufriedenheit der Mitarbeiter immens sein.

Daher sollten bei der Auswahl und Konzeption folgende Aspekte einbezogen werden:

- Welche Komponenten sind „mission critical“, d.h. ein Ausfall würde im schlimmsten Fall mein Geschäft gefährden
- Welche Ausfallzeiten sind (wenn überhaupt) zu verschmerzen
- Welche Risiken sind zu berücksichtigen
 - o Technische Defekte
 - o Ereignisse höherer Gewalt (Hochwasser, Feuer)
 - o Störungen im Anschlussbereich und im öffentlichen Netz
 - Mechanische Einwirkungen innerhalb und außerhalb des Firmengeländes (Bagger, der eine Leitung beschädigt, Blitzschlag)
 - Kommunikationsdienste, die von Dritten bezogen werden (Amtsanschlüsse, Cloud-basierte Lösungen)
- Notfallkonzepte und die damit verbundenen Ressourcen
 - o Steht ein Bereitschaftsdienst zur Verfügung, der ggf. reagieren kann, oder
 - o Muss alles automatisch passieren
 - o In welcher Zeit müssen Notfallkonzepte greifen (SLA)
- Welche Redundanzkonzepte bieten Hersteller und Integrierten an
- Sind die eingesetzten Lösungen erprobt, und gibt es objektive Erfahrungen zu Zuverlässigkeit und Verfügbarkeit
- Wer ist für die Bereitstellung einer Redundanz zuständig



Welche Komponenten sind „Mission Critical“?

Da in der heutigen Zeit die Erreichbarkeit von Unternehmen von außen ebenso wie die interne Erreichbarkeit einen besonders hohen Stellenwert haben, ist in erster Linie die Gewährleistung der Echtzeitkommunikation besonders entscheidend.

Anders als bei asynchronen Medien wie Email oder Fax, bei denen eine Verzögerung im Transport der Daten oder Unterbrechungen in der Übertragung ausgeglichen werden können und beim Empfänger kaum bemerkt werden, ist die Echtzeitkommunikation (Sprache, Video) sehr anspruchsvoll und Fehler sind sofort sicht- bzw. hörbar.

Ist ein Unternehmen oder eine Behörde telefonisch nicht erreichbar, bedeutet das Unzufriedenheit bei Kunden und Kontakten. Somit hat ein solcher Ausfall der Kommunikation direkte Auswirkungen auf die Reputation eines Unternehmens und den Geschäftserfolg. In Notfällen kann ein Ausfall der Kommunikation sogar lebensbedrohlich sein.

Eine Kommunikationslösung besteht aber dennoch meist aus verschiedenen, unterschiedlich wichtigen Komponenten. Ist das Durchschalten von Gesprächen unersetzbar, kann man ggf. auf eine Wahlhilfe durch CTI für eine bestimmte Zeit verzichten. Bei den meisten Kommunikationslösungen werden unterschiedliche Lösungsbausteine (z.B. Faxserver, CTI, Call Center, Billing) auf verschiedene Server verteilt, die z.T. sogar mit unterschiedlichen Betriebssystemen und Architekturen arbeiten. Einige dieser Dienste werden nur zentral vorgehalten, an-

dere zwar dezentral, aber ohne eine Verbindung zu einer zentralen Administration. Einfach gesagt: Je mehr unterschiedliche Server eine Lösung abbilden, umso komplexer wird es, ein vollständiges Redundanzszenario aufzubauen.

Eine Betrachtung, welche Dienste zwingend erforderlich sind und welche unter Umständen für einen bestimmten Zeitraum verzichtbar sind, ist somit unabdingbar. Auch die Schnittstellen zu sehr kritischen Dritt-Systemen wie Call Center Lösungen, Alarmservern, etc. müssen gerade in verteilten Architekturen besonders betrachtet werden.

Das alles wird vereinfacht, wenn - wie bei den Lösungen von innovaphone -, möglichst viele dieser Dienste oder Funktionen auf ein und derselben Plattform laufen, und so durch die Redundanz dieser einen Plattform nicht nur Grundfunktionen, sondern eine umfangreiche Gesamtfunktion gewährleistet werden kann.

Die innovaphone PBX beinhaltet auf einer Plattform sowohl die Gateway-Funktionen zum Anschluss an das öffentliche Netz, die kompletten Telefonanlage-Funktionen wie auch alle notwendigen Komponenten für Unified Communications, wie etwa die Präsenzanzeige, CTI-Funktionen, Video-Kommunikation und Application Sharing.

Wird also die innovaphone PBX redundant ausgelegt, bleiben im Störfall all die genannten Funktionen erhalten.

Inwieweit sind Ausfallzeiten zu verschmerzen?

Wenn man für einzelne Komponenten gänzlich auf eine Redundanz verzichtet, entsteht eine nicht zu definierende Ausfallzeit, die für ein Neuaufsetzen des Systems und (wenn hoffentlich vorhanden) das Einspielen von Backup-Daten entsteht. Sind Hardwarekomponenten betroffen, spielen auch Zeiten für die Beschaffung und Lieferung dieser Komponenten eine Rolle.

Bei solchen Entscheidungen werden in der Regel mit dem Systemintegratoren bzw. Lieferanten im Rahmen von SLAs (Service Level Agreements) sogenannte Wiederherstellungszeiten definiert. Hierbei ist es wichtig, genaustens festzulegen, was die Wiederherstellung beinhaltet und wer in welcher Form für die Datensicherung zuständig ist.

Hat man sich für den Einsatz einer redundanten Lösung entschieden, kann es, abhängig vom Redundanzkonzept, dennoch zu Ausfallzeiten kommen. Bei sogenannten Cold-Standby-Konzepten werden beispielsweise die redundanten Komponenten erst gestartet, wenn der Fehler bemerkt

wurde. Dieser Start kann Verzögerungen erzeugen, wenn z. B. der Start manuell angestoßen werden muss, und so schon eine Zeit verstrichen ist zwischen der Fehlererkennung bzw. dem Auftreten des Fehlers und dem entsprechenden Systemstart.

Diese Ausfallzeit kann deutlich verkürzt werden, wenn in einem Hot-Standby-Szenario beide Systeme parallel in Betrieb sind und im Störfall lediglich von einem auf das andere System geschwenkt werden muss. Dies erfolgt in der Regel automatisch.

Dadurch, dass sich innovaphone Plattformen einfach miteinander vernetzen lassen, können auch Redundanzszenarien problemlos im Hot-Standby-Betrieb aufgebaut werden. Im Fehlerfall werden lediglich bestehende Verbindungen getrennt, um eine Konsistenz der Datenbanken im Netzwerk sicherzustellen. Ansonsten stehen alle Funktionen unterbrechungsfrei zur Verfügung und die Mitarbeiter merken von einem Schwenk in der Regel nichts.



Verschiedene Risiken, die zu berücksichtigen sind

Technische Defekte an Hardwarekomponenten

Bei den meisten Lösungen sind entsprechende Hardwarekomponenten notwendig, um ein lauffähiges System aufzubauen. Das kann spezifische Hardware sein, ebenso auch klassische PCs oder Serversysteme. Besonders anfällig sind bei der EDV-Hardware bewegliche Teile (wie Festplatten, Lüfter) und Netzteile, sowie alle Komponenten, die hitzeempfindlich sind (CPU). Eine Reduzierung der beweglichen Teile und ein Eliminieren der Netzteile kann somit schon deutlich zur Zuverlässigkeit von Komponenten beitragen.

Die einzelnen Bauteile können zur Bildung einer Redundanz doppelt ausgelegt werden (doppeltes Netzteil, doppelte CPU). Will man aber wirklich alle Bauteile doppeln, sollte man darüber nachdenken, die gesamte Komponente - beispielsweise das TK-System - ein zweites Mal zur Verfügung zu stellen.

Die innovaphone Gateways als Hardwarebasis der innovaphone PBX sind lange im Markt bewährte, äußerst robuste Komponenten, die keine beweglichen Teile enthalten. Durch die Preisstellung der innovaphone Gateways in Verbindung mit dem flexiblen innovaphone Lizenzmodell, bei dem zusätzlich zu den vorhandenen Lizenzen pro User lediglich günstige Standby-Lizenzen erforderlich sind, ist auch der Aufbau einer physischen Redundanz für die meisten Kunden wirtschaftlich darstellbar.

Ereignisse höherer Gewalt (Hochwasser, Feuer)

Die sicherste Lösung im Falle von Ereignissen höherer Gewalt wie Hochwasser, Feuer etc. ist die Schaffung einer sogenannten Georedundanz. Mit Georedundanz wird die Tatsache bezeichnet, dass die

doppelt bereitgestellte Hardware räumlich verteilt aufgebaut wird. Damit wird Ausfällen aufgrund von lokalen Ereignissen wie Hochwasser, Feuer, Blitzschlag etc. vorgebeugt. In einem solchen georedundanten Szenario kann die Verteilung innerhalb eines Gebäudes unter Einhaltung entsprechender Brandschutzvorschriften genauso effektiv sein wie die Verteilung auf verschiedene Lokationen des Unternehmens. Hierbei sind natürlich die Vernetzung und die netzwerktechnische Verbindung der Komponenten zu berücksichtigen. Nur so können die User im Störfall auch die entferntere Komponente erreichen.

Störungen im Anschlussbereich und im öffentlichen Netz

Immer wieder wird die Kommunikation auch von Störungen beeinflusst, die nicht direkt im Verantwortungsbereich des Kunden liegen. Ein Bagger, der die Zuleitung durchtrennt, kann hier genauso zu Ausfällen führen, wie eine technische Störung im Vermittlungsknoten des gewählten Providers. Eine doppelte, räumlich getrennte Hauszuführung, entsprechend abgesicherte Leitungen des Providers oder gar eine Zwei-Provider-Strategie können hier zusätzliche Sicherheit schaffen. Abhängig vom Provider ist sicherzustellen, dass der zugeteilte Rufnummernblock weiterhin erreichbar bleibt.

Bei einer vernetzten Infrastruktur mehrerer Filialen ist bei der Planung zu berücksichtigen, wie die einzelnen Unternehmensteile erreichbar bleiben können, wenn die Zentrale nicht mehr zur Verfügung steht. Eine Variante, um höchstmögliche Sicherheit zu gewährleisten, ist der Aufbau eines Master-Slave-Szenarios.

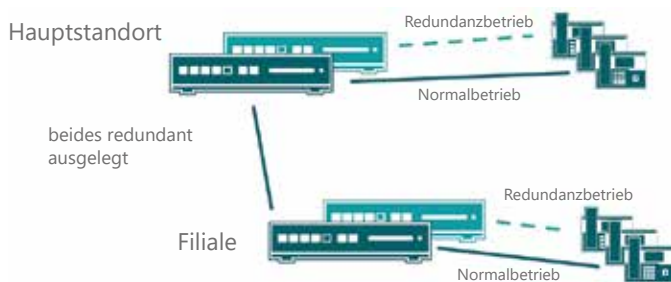
Redundanz in Master-/Slave-Systemen

Natürlich kann man jede einzelne Komponente einer Kommunikationslösung einfach doppelt auslegen. Es ist einem dabei wohl bewusst, dass die Hälfte der Komponenten (nämlich der redundante Teil) nur selten zum Einsatz kommt. Wirtschaftlich sinnvoller ist es daher, die Redundanz durch andere, gleichwertige Komponenten in einem Netzwerk zu realisieren, die im normalen Einsatzfall

ebenfalls aktiv sind. Außerdem ist dann bei Störungen wie den oben beschriebenen gewährleistet, dass die einzelnen Filialen trotzdem weiter arbeiten können. Bei IP-Telefonanlagen gibt es verschiedene Redundanzkonzepte, die realisiert werden können. Drei Varianten werden im Folgenden beschrieben.

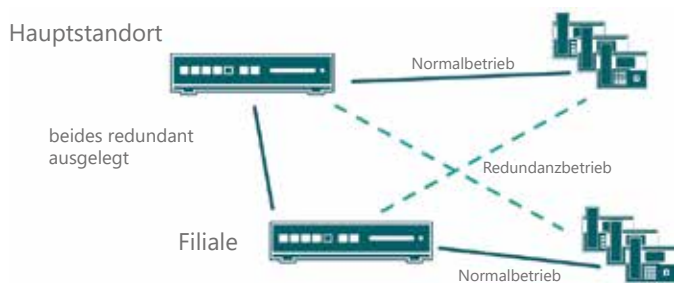
Variante 1:

Der Hauptstandort hat ein Kommunikationssystem (Master) und eine Außenstelle. Diese ist mit einem eigenen Kommunikationssystem (Slave) mit dem Hauptstandort vernetzt. Zunächst kann man jedes einzelne System redundant aufbauen. Die Telefone melden sich dann im Störfall einfach am redundanten System an.



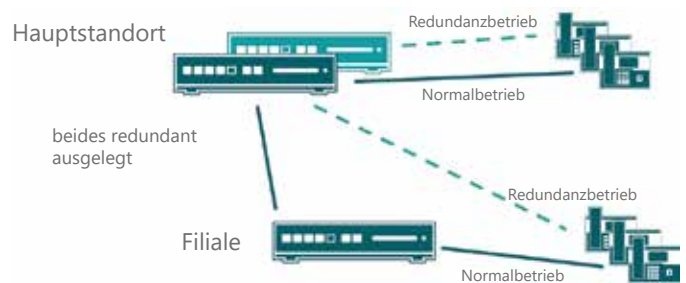
Variante 2:

Anstatt am Hauptstandort und in der Filiale jeweils ein zweites System auszubauen, kann das System am Hauptstandort bei ausreichender Dimensionierung als Redundanzsystem für die Filiale konfiguriert werden. Umgekehrt geht dies genauso, allerdings muss dann auch die Anlage in der Filiale so ausgelegt sein, dass sie im Redundanzfall die gesamte Last des Hauptstandortes übernimmt.



Variante 3:

Geht man davon aus, dass die Anlage am Hauptstandort deutlich mehr Benutzer bedient, kann es sinnvoll sein, hier doch eine physische Redundanzanlage zu installieren, also beide Systeme zu mischen.



Anders als bei vielen anderen Herstellern können mit dem innovaphone-System alle drei Redundanzvarianten realisiert werden. Mit dem Master-Slave-Konzept in einem innovaphone Netzwerk lassen sich alle Unternehmensteile so ausstatten, dass sie auch eigenständig mit sämtlichen Funk-

tionen lauffähig bleiben. Werden die Filialen mit einer separaten Trunkleitung ausgestattet, ist auch die Erreichbarkeit (ein- und ausgehend) sichergestellt. Besonders wichtig ist dies auch für die Möglichkeit, Notrufe absetzen zu können.

Weitere Redundanzkonzepte und -varianten

Die oben genannten Redundanzkonzepte und Szenarien lassen sich mit eigenen Komponenten beliebig kombinieren und erweitern. Zusätzlich gibt es aber noch zahlreiche weitere Optionen, von denen noch zwei weitere im Folgenden angesprochen werden sollen.

Virtualisierung

Virtualisierte Umgebungen bieten den Vorteil, dass verschiedenste Systeme für unterschiedliche Einsatzbereiche auf einer standardisierten EDV-Hardware eingesetzt werden können. Die Virtualisierungsumgebung (z.B. VMWare oder Hyper-V) bietet dann wiederum eigene Mechanismen an, um eine Hochverfügbarkeit zur Verfügung zu stellen und die verschiedenen Systeme zu verwalten.

Die Umschaltung auf eine weitere Instanz erfolgt in der Regel innerhalb von Sekundenbruchteilen ohne Verlust. Wichtig ist es sicher zu stellen, dass die Lösungen, die man auf der virtuellen Plattform implementiert, auch die entsprechenden HA- (High Availability-) Mechanismen unterstützen.

Cloud-Lösungen

Cloud-Lösungen werben mit hoher Verfügbarkeit und der Reduktion von Betriebskosten. Man kann in der Tat davon ausgehen, dass seriöse Betreiber von Cloud-Plattformen entsprechende Vorkehrungen in ihren Datacentern treffen, um eine größtmögliche Ausfallsicherheit zu erreichen.

Häufig sind diese Maßnahmen umfangreicher und hochwertiger, als es sich einzelne Unternehmen leisten würden, können hier schließlich die getätigten Investitionen auf deutlich mehr Kunden und Nutzer umgelegt werden. So profitieren alle Seiten von diesen Technologien.

Trotz dieser ohnehin hohen Sicherheit werden auch Lösungen angeboten, bei denen eine lokale Redundanz Grundfunktionen oder auch die Gesamtfunktion zur Verfügung stellen kann. Dazu kann vor Ort eine Komponente installiert werden, die die lokale Kommunikation verwaltet, aber auch bei Ausfall der Cloud-Verbindung einen lokalen Amtszugang verwendet. Andererseits gibt es auch Anbieter, die den umgekehrten Weg gehen und ihre Cloud-Infrastruktur als Redundanz für lokale Installationen anbieten.

innovaphone bietet als Ausstatter von Cloud-Plattformen zahlreicher Service-Provider nicht nur die bekannt umfangreichen UC-Funktionen für alle Nutzer. Mit den oben beschriebenen Möglichkeiten lassen sich durch eine bedarfsorientierte Kombination aller Möglichkeiten sämtliche Sicherheitsbedürfnisse der Kunden erfüllen - sei es durch ein besonders abgesichertes System in der Cloud oder durch die Bereitstellung lokaler Gateways als lokale Redundanz.

Zusammenfassung

Echtzeitkommunikation ist heute für die meisten Unternehmen ein Schlüsselfaktor für betriebswirtschaftlichen Erfolg. Abhängig von Gefährdungssituationen und Risiken, aber auch abhängig von der technischen Ausrichtung und letztlich vom Budget gibt es zahlreiche Varianten, die Kommunikation ausfallsicher zu gestalten.

innovaphone beweist täglich bei vielen namhaften Kunden, dass sichere und zuverlässige Kommunikation machbar ist - und das mit überschaubarem technischen und wirtschaftlichen Aufwand.

CHECKLISTE

für eine stabile und sichere Kommunikationslösung

Als Hilfestellung für die Planung einer sicheren Kommunikationslösung haben wir die folgende Checkliste erstellt:

Welche Ausfallszenarien sind zu berücksichtigen:

- Feuer / Hochwasser
- Externe Schäden (Zuleitung)
- Überhitzung
- Stromausfall -> Dauer
- Technische Schäden an Servern oder anderen Komponenten

Welche technischen Systeme/Redundanzen sind vorzusehen:

- Stromversorgung
 - o USV
 - o Doppeltes Netzteil
- CPU
- Festplatten / Dopplung / automatisiertes Backup
- Netzwerkkarten / Switches / Router
- Redundanz via Virtualisierungsumgebung (HA / FT)
- Systemdopplung
 - o Hot- / Cold Stand-by
 - o mit welchen Ausfall- / Umschaltzeiten ist zu rechnen
 - o Was genau passiert beim Greifen der Redundanz

Welche Kommunikations-Dienste müssen immer zur Verfügung stehen bzw. abgesichert werden (Backup)

- Basistelefonie intern / eingehend / abgehend
- Notruf
- Vermittlungsplatz
- Call Center / Contact Center / Hotline
 - o Telefonie / Chat / Email
- CTI / Wählhilfe
- Videokommunikation
- Application sharing
- CRM
- ERP
- Troubleshooting System
- Alarmierungssysteme
- weitere

Wie findet eine Überwachung der Komponenten / Alarmierung statt

- Netzwerk-Monitoring
- Alarmierungen
- SNMP
- Alarm/Event Mail-Benachrichtigung
- Logging von Konfigurationsänderungen



INNOVAPHONE

Das ist „Pure IP Communications made in Germany“ – und das seit jeher.

Schon seit ihrer Gründung im Jahr 1997 hat sich die innovaphone AG auf die Entwicklung und Herstellung von reinen IP-Kommunikationssystemen spezialisiert. Diese langjährige Erfahrung und intensive Ingenieursarbeit macht die innovaphone PBX zu einer so einzigartigen und durchdachten IP-Telefonie- und Unified Communications-Lösung – auch aus der Cloud.

Das ist noch „echter inhabergeführter Mittelstand“.

Das Technologieunternehmen ist zu 100 % eigenfinanziert und die Gesellschafter bilden gleichzeitig das Management-Team. Durch diese Gesellschafterstruktur wurde und wird das international ausgerichtete, unabhängige Unternehmen nachhaltig geprägt und hat sich als verlässlicher Partner im europäischen Markt etabliert.



Copyright © 2017 innovaphone® AG. (E 12/2017)
Irrtümer, Liefermöglichkeiten und technische Änderungen vorbehalten.



GET IN TOUCH

innovaphone AG
Böblinger Str. 76
71065 Sindelfingen

Tel. +49 7031 73009-0
Fax +49 7031 73009-9

info@innovaphone.com
www.innovaphone.com