



Gesundheitswesen

Das Gesundheitswesen entwickelt sich zunehmend zu einer offenen und verteilten Struktur im Sinne des „Shared Care“. Effizienzsteigerungen werden maßgeblich vom Einsatz aller Spielarten der elektronischen Datenverarbeitung beeinflusst. Neben organisatorischen Maßnahmen ist der Einsatz von IT-Sicherheits-Systemen unabdingbar zur Erreichung des erforderlichen Sicherheitsniveaus. Dabei sind insbesondere die hohen Anforderungen an Integrität und Vertraulichkeit von Personendaten zu gewährleisten. LiSS Security Systeme erfüllen die komplexen Sicherheitsanforderungen im Gesundheitswesen in besonderem Maße.

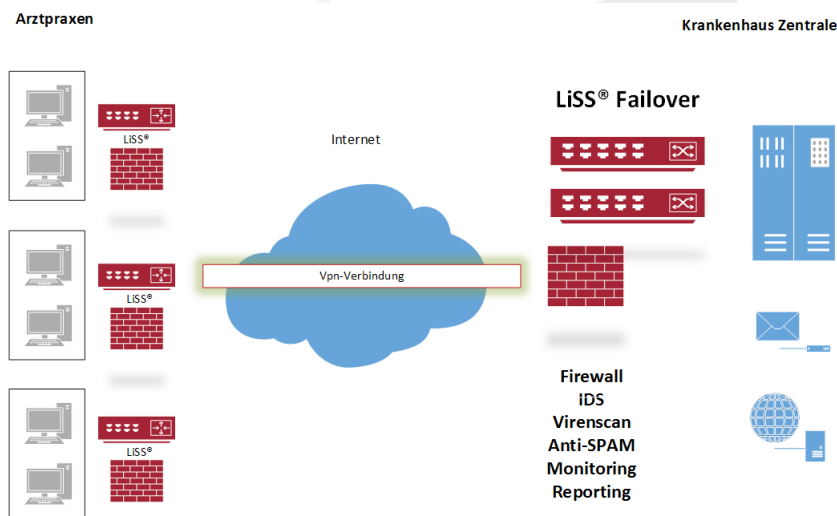
Vorteile von LiSS Security Systemen

- Kompatibel zu eHealth-Standardanwendungen
- Bundesweites Servicenetzwerk
- Made in Germany (no backdoors)
- Kostenfreier Support

Einsatzgebiete von LiSS Security Systemen

Klinik - Praxis - Mobiler Arbeitsplatz

- Sichere Kommunikation im Netzwerk oder über das Internet, drahtgebunden oder via Funk
 - zwischen Facharzt - Krankenhaus
 - zwischen Fachabteilungen
 - von externen Dienstleistern
- Physische und logische Entkopplung von Netzwerken, beispielsweise:
 - separate Verwaltung radiologischer Systeme
 - Schutz von Patientendaten
 - Entkopplung verschiedener Sicherheitszonen
- Analyse der Datenströme und Schutz vor unerwünschten Inhalten
- Umsetzung kontextbezogener Zugriffsberechtigungen
- Erkennung von SPAM-E-Mails
- Webfilterung (Virus, Content etc.)
- Optionen:
 - Hochverfügbarkeit/Redundanz
 - Full-Management
 - Vor-Ort-Service





Produktvorteile der LiSS series auf einen Blick:

● **Mehrstufiger Schutz der Infrastruktur (Firewall)**

Die Firewall entkoppelt Netzwerke und ermöglicht den Aufbau unterschiedlicher Sicherheitszonen, in der die besonders schutzbedürftigen Systeme gegen andere Netze (z. B. Internet, LAN) abgeschirmt sind. Dadurch können im Haus sogar „unsichere“ Web-Services genutzt werden, ohne die eigene Infrastruktur zu gefährden.

● **Sichere externe Kommunikation (VPN Modul)**

Die sichere Anbindung externer Partner und Telearbeiter erfolgt nach dem vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlenen IPSec-Standard.

● **Problemlose Integration (Single Sign On)**

Dank der Nutzungsmöglichkeiten von vorhandenen Verzeichnisdiensten (z. B. Active Directory) entfällt für die Mitarbeiter zum einen die Notwendigkeit der Mehrfachanmeldung, zum anderen erleichtert dies die Umsetzung der eigenen Sicherheitspolitik.

● **Inhaltsfilter (Anti-Virus, Anti-SPAM, Internetrichtlinie)**

Unerwünschte und schädliche Inhalte werden während der Internetnutzung erkannt und unterbunden. Nutzer-Rechte können individuell oder gruppenspezifisch vergeben werden. Die Anti-SPAM-Technologie entlastet Ihre Mitarbeiter spürbar.

● **Hochverfügbarkeit (Redundanz)**

Services und Systeme müssen für Mitarbeiter dauerhaft verfügbar sein. Zur Kompensation eventueller Hardwareausfälle können die Geräte redundant ausgelegt werden. Im Havariefall erfolgt die Umschaltung vollautomatisch.

● **Kostenreduktion (Policy Based Routing)**

Datenströme können entsprechend ihrer Priorität über verschiedene Internetzugänge geleitet werden (bspw. Internetzugriffe der Nutzer über eine kostengünstige Flatrate, wichtige Applikationen dagegen über eine Standleitung mit garantierter Bandbreite). Bei Ausfall einer Verbindung kann automatisch auf die noch verfügbare Verbindung geschwenkt werden.

● **Datenintegrität (Made in Germany)**

Im Rahmen einer Selbstverpflichtung garantiert Telco Tech, dass alle LiSS Security Systeme grundsätzlich ohne versteckte Zugangsmöglichkeit (backdoor) hergestellt und vertrieben werden.

● **Management/Service (Management Services)**

Für alle LiSS Security Systeme steht umfassender deutschsprachiger Support zur Verfügung. Telco Tech bietet neben dem kompletten Management auch die Möglichkeit, verschiedene Service-Level und Verfügbarkeitsgarantien zu kombinieren.