

Sicherer Online-Zugang

für die Telematikinfrastuktur



Synchronizing Healthcare



CompuGroup
Medical

Sicherer Online-Zugang für die Telematikinфраstruktur

Der Anschluss an die Telematikinфраstruktur (TI) ist sicher und der Datenverkehr mit Patientendaten geschützt. Unabhängig davon ist ein zusätzlicher Schutz des Online-Zugangs Ihrer Institution unerlässlich und gemäß den Sicherheitsstandards u. a. der Landesorganisationen und des Bundesamts für Sicherheit in der Informationstechnik „BSI“ vorgeschrieben, denn Ihre Institution geht auch ins Internet. Wir helfen Ihnen sich gemäß den Vorgaben des BSI noch besser gegen Cyberangriffe zu schützen und bieten Ihnen den „Sicheren Online-Zugang für die Telematikinфраstruktur“ in vier Varianten:

Sicherer Online-Zugang – Hoher Schutz

Diese Zugangsvariante bietet einen hohen Schutz vor Cyberangriffen. Der Zugriff auf das Internet erfolgt zentral geschützt durch Firewalls, Virens Scanner und Contentfilter sowie dezentral geschützt durch Firewalls und Paketfilter. Anwendungen und Dienste können damit hochsicher betrieben werden, da der Datenstrom nicht bzw. geschützt über das Internet läuft und somit nicht mitgehört werden kann. Anfragen an das Internet werden zuverlässig geprüft und Cyberangriffe abgewehrt. Das dazugehörige TELEMED-E-Mail-Postfach besitzt einen Spam-Filter. Die CGM-Mehrwertdienste sind erreichbar.

DIE SCHUTZSTUFE „HOCH“

BIETET SCHUTZ VOR:

- Zugriff auf Router durch Ausnutzung von Schwachstellen
- Zugriff auf das Institutionsnetz einschl. Patientendaten
- DoS (Denial of Service)-Attacken – Nichtverfügbarkeit des Online-Zugangs
- Ausspionieren von Schwachstellen durch öffentliche Sichtbarkeit
- Spam
- × Phishing, Virenangriffen und Spyware durch E-Mails (eingeschränkt)
- × Virenangriffen und Spyware beim Surfen (eingeschränkt)

Sicherer Online-Zugang – Sehr hoher Schutz

Die Stufe „Sehr hoch“ bietet den höchsten Schutz vor Cyberangriffen. Die TELEMED Firewall schützt uneingeschränkt vor Phishing, Spyware und Viren durch E-Mails oder beim Surfen. Diese wird zusätzlich im Institutionsnetz eingesetzt und erhöht den Schutzgrad durch zusätzliches URL- & Contentfiltering, somit ist ein sehr hoher Schutz gegeben. Die CGM-Mehrwertdienste sind weiter erreichbar.

DIE SCHUTZSTUFE „SEHR HOCH“

BIETET SCHUTZ VOR:

- Zugriff auf Router durch Ausnutzung von Schwachstellen
- Zugriff auf das Institutionsnetz einschl. Patientendaten
- DoS (Denial of Service)-Attacken – Nichtverfügbarkeit des Online-Zugangs
- Ausspionieren von Schwachstellen durch öffentliche Sichtbarkeit
- Spam
- Phishing, Virenangriffen und Spyware durch E-Mails*
- Virenangriffen und Spyware beim Surfen

* Webmail: Schutz erfolgt während des Zugriffs im Browser; E-Mail-Client: Schutz über lokale CGM Endpoint-Protection; bzw. Schutz über TELEMED Firewall, die Funktionen werden über Updates fortlaufend bereitgestellt.

Schutzstufen

des sicheren Online-Zugangs

SEHR HOHER SCHUTZ – TELEMED Firewall



Upgrade auf Sicherheitsstufe „Sehr hoch“ – Realisierung über TELEMED Firewall

- TELEMED Firewall wird zusätzlich ins Institutionsnetz integriert
- Bei TELEMED All-IP und TELEMED Trusted Internet Flat zusätzlich einsetzbar
- Zusätzlicher Schutz vor Phishing, Spyware und Viren auch bei verschlüsselten E-Mails*

*Voraussetzung ist der Einsatz der SSL-Inspection der TELEMED Firewall.

HOHER SCHUTZ – TELEMED All-IP



DSL/ISDN-Umsteiger und All-IP-Neuanschluss – Realisierung über TELEMED All-IP

- Sicheres Intranet von TELEMED
- Nur TELEMED-IP-Adresse im Internet sichtbar, **Ihre Institution kann von Angreifern nicht identifiziert werden**

HOHER SCHUTZ – TELEMED Trusted Internet Flat



Bereits vorhandener All-IP/DSL-Anschluss – Sicher online über TELEMED Trusted Internet Flat

- Zusätzlicher Schutz für bereits vorhandenen All-IP/DSL-Anschluss
- Gesicherter VPN-Tunnel zur sicheren Internetnutzung über bereits vorhandenen Provider in Ihrer Institution (Fremdprovider)
- Ausspionieren Ihrer Institution wird durch LANCOM-Router verhindert

BASISSCHUTZ – TELEMED Secure Internet Service Flat



Bereits vorhandener All-IP/DSL-Anschluss – Online-Zugang über TELEMED Secure Internet Service Flat

- Gesicherter VPN-Tunnel zur sicheren Internetnutzung über bereits vorhandenen Provider in Ihrer Institution (Fremdprovider)
- Angreifbares öffentliches Netz mit öffentlicher IP-Adresse wird weiterhin verwendet
- Die Nutzung von CGM-Mehrwertdiensten ist nur bei zusätzlicher Beauftragung möglich

Installationskomponenten für den sicheren Online-Zugang

Schutzniveau	Internetanschluss vorhanden?			LANCOM Router	TELEMED Firewall	LANCOM Switch (optional)	Fernzugriff/Heimarbeit (optional) TELEMED Mobile Praxis Center
	Nein: TELEMED All-IP Zukunftssicherer All-IP/DSL-Anschluss mit TELEMED-Zugangsdaten (gilt auch für Umsteiger von vorhandenen Providern)	Ja: TELEMED Trusted Internet Flat Sicherer VPN-Tunnel über das öffentliche Netz direkt in das sichere TELEMED-Netz, für Institutionen die bereits einen All-IP/DSL-Anschluss haben.	Ja: TELEMED Secure Internet Service Flat Sicherer VPN-Tunnel SIS über das öffentliche Internet (nur in Verbindung mit der Telematikinfrastruktur bzw. dem VPN-Zugangsdienst buchbar)				
Basisschutz			✓				✓
Hoher Schutz	✓	✓		✓		✓	✓
Sehr hoher Schutz	✓	✓		✓	✓	✓	✓

Schutzniveau	Alternative , wenn kein All-IP-Zugang technisch realisierbar -> TELEMED LTE (soweit verfügbar)		
	LTE Flat Sichere Online-Anbindung über TELEMED LTE-Datenzugang (ohne Telefonie)	LANCOM LTE-Router	Firewall TELEMED Firewall
Hoher Schutz	✓	✓	
Sehr hoher Schutz	✓	✓	✓

Sprechen Sie uns zur Herstellung eines sicheren Online-Zugangs gerne an.

CompuGroup Medical Deutschland AG
Geschäftsbereich TELEMED
Maria Trost 21 | 56070 Koblenz
T +49 (0) 261 8000-2007
F +49 (0) 261 8000-2029
info@telemed.de

cgm.com/ti

CGMCOM/7026_296_VOR_TL_1019_RRH | Version: 1.3 | Stand: Oktober 2019

Synchronizing Healthcare



**CompuGroup
Medical**