Angemessene Lösungen erfordern Differenzierung der Szenarien

# Sicherheitsbetrachtungen zum SIP-Trunking

Der Artikel liefert einen Überblick zu den Fragen und Maßnahmen des Risikomanagements, die ein Unternehmen beim Wechsel seines Sprachanschlusses auf einen SIP-Trunk berücksichtigen sollte.

Autor: Dipl.-Ing. Andreas Steinkopf

## Einführung

Unternehmen und Organisationen haben heute viele Compliance-Regeln und -Normen zu beachten. Beim Thema Sicherheit kommt im Allgemeinen Fall die ISO 31000 als Antwort daher und gibt ein Regelwerk zum Risikomanagement vor. Telefonie gehört insbesondere durch die Computer-Telefonie-Integration (CTI) längst in die Welt der Informationstechnologie, genauso wie das IP-Protokoll und somit auch ein darauf aufbauender SIP-Trunk, der im Zuge des All-IP-Wandels den klassischen ISDN-Anlagenanschluss ablöst. Dies führt zum spezielleren Fall der Informationssicherheit und somit zur ISO-27000-Normenreihe, die ein Informationssicherheits-Managementsystem (ISMS) anbietet, sowie zum BSI-»IT-Grundschutzkatalog«, der kompatibel zur ISO 27001 ganz ähnliche Anforderungen beschreibt. Die ISO 31000 besagt, dass die Geschäftsleitung in einem Top-Down-Verfahren die Risiken identifizieren, analysieren und bewerten (lassen) muss. Ist die Kombination aus Eintrittswahrscheinlichkeit und potenziellem Auswirkungsschaden eines Risikos – wie insbesondere einer Sicherheitslücke – hinreichend groß, muss geplant werden, wie die Eintrittswahrscheinlichkeit und/oder der Schaden zu reduzieren ist, um ein vertretbares Restrisiko zu erreichen.

Wegen fehlender, verlässlicher Statistikinformationen zur Eintrittswahrscheinlichkeit oder Schadenshöhe tun sich viele Unternehmen und Organisationen jedoch schwer, eine eigenständige Risikoanalyse zu erstellen. Daher wird diese beim BSI-Grundschutz pauschaliert und der Grundschutzkatalog nennt Standardgefährdungen und Standardsicherheitsmaßnahmen für typische und verbreitete IT-Systeme und Netze. Allerdings soll auch hier eine IT-Strukturanalyse erfolgen, deren Ausgangsbasis im Kommunikationsumfeld der Netztopologie-Plan sein sollte. Pauschaliert wird auch der Schutzbedarf, der in die drei Schutzbedarfskategorien »normal«, »hoch« und »sehr hoch« unterteilt wurde.

Die hier zu erreichende Informations- bzw. Kommunikationssicherheit ist durch zwei englische Wörter besser aufgeschlüsselt: »Safety« steht für »Betriebssicherheit« im Sinne von Verfügbarkeit und Vermeidung von finanziellem Schaden. »Security« steht für die eigentliche, sichere Kommunikation, die wiederum auf Integrität, Authentizität und Vertraulichkeit beruht.

Dies aufgezeigt, erschließen sich Aufbau, Inhalt und Fachbegriffe der folgenden Abschnitte.

Inhalt



## Kostensicherheit

Die mit Abstand höchste Kombination aus Eintrittswahrscheinlichkeit und potenzieller Schadenshöhe ist nach der Erfahrung des Autors bzw. eines Internet-Telephony-Service Providers (ITSP) ein **Fraud-Fall** (engl. für Betrug), weil im Umfeld der TK-Anlage bzw. des SIP-Trunks ein Passwort nicht gut ausgewählt oder ein voreingestelltes oder leeres Passwort nicht geändert wurde (siehe auch M2.11 in **[BSI01]**). Eine derartige Unterlassung ermöglicht es Betrügern, über die TK-Anlagen-Administrations- oder Anwenderkonsole inkl. Fernwartungszugang, über ein Endgeräte-Login, über Voice-Mailboxen und auch über die SIP-Trunk-Registrierung die TK-Anlage bzw. den Sprachanschluss zu hacken und teure Verbindungen – meist zu Servicerufnummern im Ausland – zu generieren.

Aber auch mit sicheren TK-Passwörtern können Hacker moderne TK-Anlagen hacken, wenn diese Softwaresicherheitslücken – namentlich in ihrem Betriebssystem – aufweisen. Hier gilt es also zuvorderst, alle »normalen« Sicherheitsmaßnahmen für einen Server mit IP-Verbindungen zu ergreifen, wie z. B. regelmäßige Updates und natürlich sichere Administratoren-Passwörter.

Telefoniespezifisch sind sowohl auf der ITSP- als auch zusätzlich auf der Kundenseite weitere Maßnahmen ratsam:

Auf der Seite des Next Generation Networks (NGN) kann der SIP-Trunk vom ITSP für ausgehende Verbindungen zu Service- und Auslandsrufnummern gesperrt werden.

Quelle: Mitgliedermagazin „VAF-Report“;
Hrsg.: VAF Bundesverband Telekommunikation e.V., März 2016. www.vaf-ev.de

Und der ITSP kann eine allgemeingültige Fraud Prevention und Detection implementieren, die neben verschiedenen Anomalie-Screenings vielfach darauf beruht, dass er pro gefährdeter Rufnummerngasse Schwellwerte für das Verbindungsvolumen definiert und überwacht und im Alarmfall mit geringer Verzögerung geeignete Gegenmaßnahmen – wie eine SIP-Trunk-Abschaltung – ergreift. Auf der Kundenseite können zusätzlich Kundenindividuellere bzw. -spezifischere Gefahrenmuster und Schwellwerte implementiert, überwacht und Ereignisse sofort reportet werden. Dies entweder in der TK-Anlage selbst oder in einem vorgeschalteten Enterprise Session Border Controller (E-SBC), da sich nur diese beiden Komponenten hinreichend auf der SIP-Protokoll-Applikationsebene auskennen.

## Betriebssicherheit

Wie Ausfälle der letzten Monate im noch »jungen« NGN der Deutschen Telekom gezeigt haben, hängt die Betriebssicherheit auf der ITSP-Seite stark davon ab, dass unter Einbeziehung der Systemlieferanten alle Systemkomponenten auch im Detail aufeinander abgestimmt sind, dass das NGN durchgängig mit stabilen und redundanten Komponenten aufgebaut ist und dass ein umfassendes System- und Change Management etabliert ist und optimiert wurde. Dies braucht Zeit, sprich das Beschreiten einer »Lernkurve«. Ganz ähnlich auf der Kundenseite: Auch hier muss gelernt werden, wie die Ausfallwahrscheinlichkeit des oder der neuen TK-Anlagenserver(s) und des IP-Netzwerks mit geeigneten Managementmaßnahmen – z. B. des BSI-Grundschutzkataloges – hinreichend gesenkt werden kann.

Ist eine **hohe bis sehr hohe Verfügbarkeit** gefordert, kann das Ausfallrisiko der IP-Telefonie weiter gesenkt werden, indem der SIP-Trunk, die IP-Standortanbindung und die TK-Anlage bzw. die Anlagenserver redundant ausgelegt werden. Dies wird in **Bild 1** im Detail dargestellt.

**Verfügbarkeitsstufe 1** mit einem TK-Anlagenserver (im Bild TK-Anlagenserver 1) und einer Standortanbindung (im Bild CPE 1): Meist ohne Aufpreis für den Kunden kann der ITSP eine erhöhte SIP-Trunk-Verfügbarkeit liefern, indem er ortsredundante Session Border Controller (SBC) installiert. Der SIP-Trunk wird dann im »Dual Homing«-Modus betrieben: Im Normalfall baut die TK-Anlage den SIP-Trunk zum ersten SBC des ITSP auf (im Bild SIP-Trunk 1 zu SBC-Cluster Nord). Fällt dieser SBC aus, baut die TK-Anlage den SIP-Trunk zum redundanten SBC auf (im Bild SIP-Trunk 2 zu SBC-Cluster Süd). Schon etwas teurer, aber die Ausfallwahrscheinlichkeit gemäß SLA (Service Level Agreement) des Zuführungsproviders ein weiteres Stück senkend, ist die **Verfügbarkeitsstufe 2**, weiterhin mit einem TK-Anlagenserver an einem Standort, aber nun mit zwei Standortanbindungen (im Bild CPE 1 und CPE 2): Fällt hier die primäre Standortanbindung (an CPE 1) aus, übernimmt der sekundäre Router (CPE 2) automatisch die Kommunikation, indem er über eine VRRP- oder HSRP-Verbindung (VRRP = Virtual Router Redundancy Protocol gemäß RFC 5798, HSRP = Hot Standby Router Protocol von Cisco) mit dem primären Router kommuniziert. Dies wird meist einfach »IP-Backup« genannt.

Verschiedene TK-Anlagenhersteller bieten eine optionale Redundanz für ihre TK-Anlagenserver an: In dieser **Verfügbarkeitsstufe 3** melden sich zwei – oder mehr – Anlagenserver der gleichen TK-Anlageninstanz für den gleichen logischen SIP-Trunk beim ITSP an (im Bild Anlagenserver 1 und 2) und können so beide abgehende Verbindungen aufbauen. Eingehende Verbindungen werden den Servern gleichverteilt zugestellt, die aus Sicht der ITSP-SBC »online« sind, also antworten. Die Server können sogar an verschiedenen Standorten stehen (im Bild Zentralgebäude 1 und 2), müssen sich aber auch dann permanent synchronisieren.

Mit dieser Stufe hat man alle »Single Points of Failure« ausgemerzt und eine Ortsredundanz auf ITSP- und Kundenseite geschaffen. Dies geht deutlich weiter als das ISDN-Leistungsmerkmal »Mehrfachabstützung«, mithilfe dessen bei Ausfall einer Vermittlungsstelle nur ein Teil der ankommenden Gespräche über die zweite Vermittlungsstelle abgewickelt werden konnte. Zudem unterstützten viele TK-Anlagen dieses Merkmal nicht. Und wenn man es schaffte, die Beschränkung auf ein Ortsnetz hinter sich zu lassen, konnten Taktprobleme zu Störungen führen.

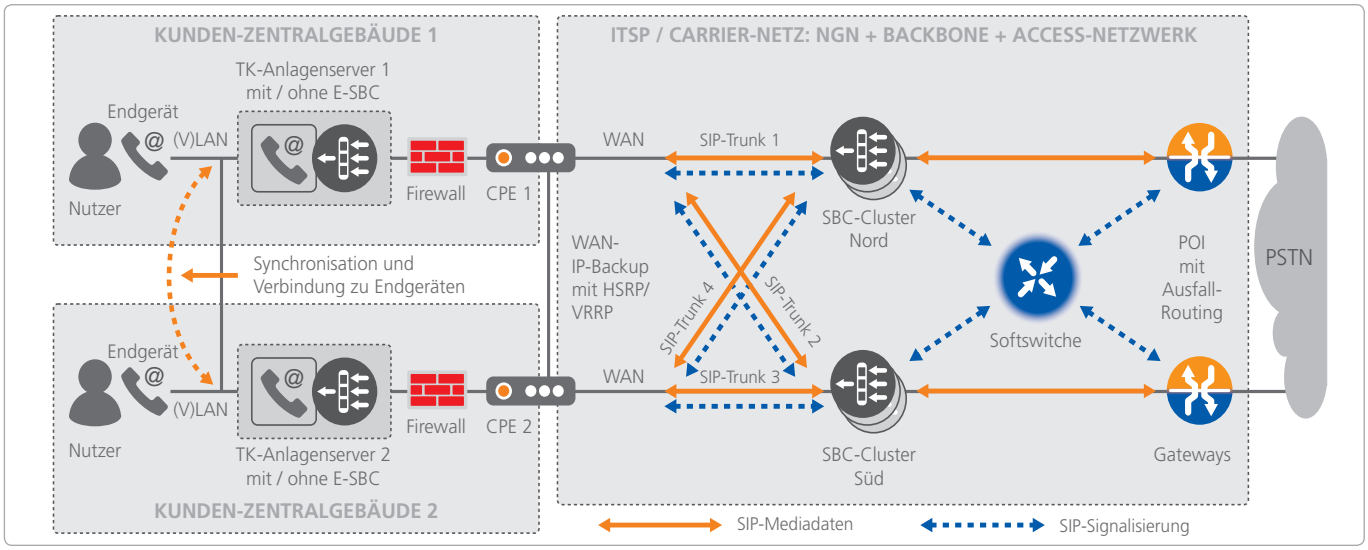



**Bild 1:** Mit einem SIP-Trunk kann eine durchgängige Redundanz der Sprachanbindung realisiert werden.

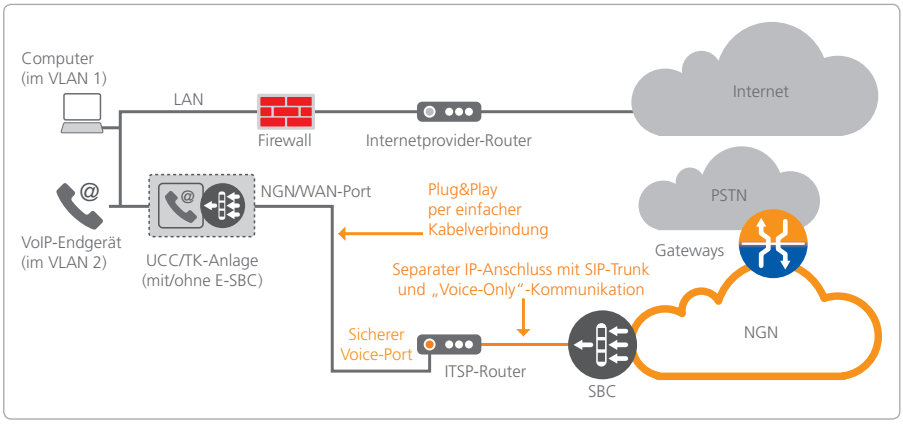



**Bild 2:** Eine klare Trennung der Daten- und VoIP-Netze sowie mehr Redundanz ergeben sich mit einem separaten »Voice-only«-Anschluss.

## Internetsicherheit

Alle über IP angebundenen Geräte, die direkt oder indirekt mit dem Internet verbunden sind, unterliegen dem Risiko kaum überschaubarer, diverser Angriffsszenarien, sodass auf der anderen Seite diverse Gegenmaßnahmen, wie der Einsatz einer Firewall, dieses Risiko senken sollten. Im VoIP-Umfeld wird zusätzlich empfohlen, **Daten- und VoIP-Netz zu trennen.** Im Kunden-LAN erfolgt dies am besten auf Layer 2 mittels VLAN-Technologie (Virtual Local Area Networks) im Ethernet-Switch. Bei erhöhten Sicherheitsanforderungen wird sogar empfohlen, diese Netze physikalisch zu trennen (siehe auch M2.376 in **[BSI01]**), was den Aufwand im LAN mindestens verdoppelt.

Viele Hersteller haben gelernt, ihren IP-basierten TK-Anlagen einen separaten **NGN- bzw. WAN-Ethernet-Port** zu spendieren. Dieser kann entweder in die »Haupt-Appliance«, einen separierten Mediation-Server oder einen vorgeschalteten E-SBC integriert sein. Auf der ITSP-Seite wurde ganz Ähnliches gelernt: Auch hier können einige Anbieter schon einen separaten **Voice-Ethernet-Port am Access-Router** liefern. Dieser wird – z. B. mittels Access-Control-Liste (ACL) – auf dem Router so konfiguriert, dass er ausschließlich mit den Voice-Komponenten des ITSP-NGN, also namentlich seinen SBC, kommunizieren kann. Da diese nur bereinigte SIP-Kommunikation passieren lassen, erreicht auch den Voice-Port des Access-Routers ausschließlich diese – nicht jedoch die gefährliche Internetkommunikation.

Beides zusammen ergibt nun die Möglichkeit, auch auf der SIP-Trunk-Seite die Netze zu trennen: Wie in **Bild 2** ersichtlich, kann ein vom Internetanschluss völlig getrennter **»Voice-only«-SIP-Sprachanschluss** direkt mit einem einfachen Kabel wie bei ISDN mit der IP-TK-Anlage verbunden werden, was den Installationsaufwand deutlich reduziert. Somit werden nicht nur die Netze höchst sichtbar getrennt, sondern auch die Verantwortungsbereiche: Das TK-Anlagen-Fachunternehmen braucht sich wegen des SIP-Trunks weder mit dem Firewall-Verantwortlichen abzustimmen, noch beim Internetprovider um eine Sprachdatenpriorisierung zu ersuchen.

Bei diesem »Single Play«-Anschluss wird also im Vergleich zum »Dual Play«-Anschluss der Internetdienst abgeschaltet, was der ITSP zum Anlass nehmen kann, ihn günstiger als einen Dual-Play-Anschluss – mindestens jedoch nicht teurer als einen ISDN-Anschluss – anzubieten.

Gleichwohl müssen zwei IP-Standortanbindungen bezahlt werden. Dies spricht aus Gründen der Anbindungskosten für die im **Bild 3** dargestellte **ITK-konvergentere Sprach/Datenanbindung**. Durch die Verbindung zum Internet steigt zwar das Risiko eines Router-Angriffs bzw. -Ausfalls ein wenig, aber durch die Trennung von Daten- und Voice-Port und die Separierung des VoIP-Traffics über die SBC des ITSP bleibt eine logische Trennung der Traffic-Arten erhalten. Und der Schutz vor Internetangriffen über den Voice-Port.

Ob bei den Szenarien der Bilder 2 und 3 vor bzw. mit der TK-Anlage ein E-SBC zu installieren ist, sei der Diskussion des TK-Anlagenherstellers und -Systemintegrators mit seinem Kunden bzw. den Betrachtungen des Fachbeitrags von Mathias Hein inklusive Plädoyers auf S.16 dieser Ausgabe überlassen.

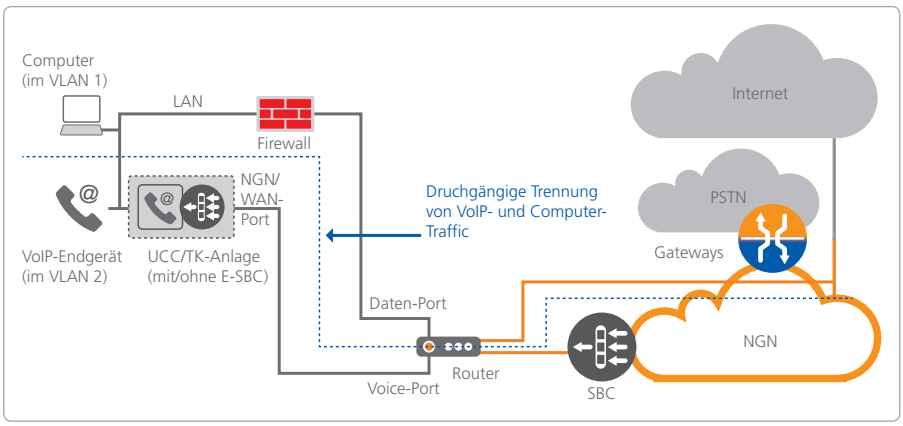



**Bild 3:** Auch die ITK-konvergente Standortanbindung separiert Internet- und VoIP-Traffic.

## Kommunikationssicherheit

Welche technischen Protokolle verwendet werden sollten, um die Kommunikationssicherheit für einen SIP-Trunk zu erhöhen, ist weder von der Empfehlungs- noch der Hersteller/ITSP-Seite strittig: Wie in **Bild 4** (siehe grüne 1) gezeigt, kann die Vertraulichkeit, Integrität und Authentizität der Mediendaten auf dem Layer 5 des ISO/OSI-Schichtenmodells mit dem **Secure Real Time Protokoll** (SRTP) deutlich erhöht werden. Es ist sinnvoll, SRTP mit dem **Transport Layer Security Protocoll** (TLS) auf dem Layer 4 zu kombinieren (siehe grüne 2), das zusätzlich die Integrität und Authentizität der SIP-Signalisierung erhöht. Diese beiden optionalen SIP-Trunk-Protokolle erhöhen nur die Kommunikationssicherheit des SIP-

Trunks. Gerade wenn eine Organisation mehrere Standorte mit IP vernetzen will, empfiehlt es sich, dies mit einem IP-VPN zu tun, bei dem die IP-Kommunikation aller Anwendungen über private, nicht aus dem Internet zu erreichende IP-Adressen erfolgt. Ein IP-VPN kann komfortabel – weil Netz-basiert – vom ITSP gebaut und geliefert werden, indem dieser ein **Multi-Protocol-Label-Switching-VPN** (MPLS-VPN, siehe grüne 3 auf Layer 2) für den Kunden aufbaut. Auch der SIP-Trunk kann mit dem IP-VPN abgesichert werden, indem der ITSP eine direkte und private Verbindung zwischen dem Kunden-IP-VPN und seinen SBC herstellt.

Alternativ oder sogar auch zusätzlich kann ein **IPsec-VPN** (siehe grüne 4) aufgebaut werden, um alle Daten zwischen den Kundenstandorten und dem SIP-Trunk nicht nur »abzuschotten«, sondern auf Layer 3 auch zu verschlüsseln. Diese Verschlüsselung erfolgt für jeden Kundenstandort im Access-Router, was mit der Standortanzahl schnell ansteigend zu einem hohen Provisionierungs- und Managementaufwand führt. Der Aufwand lässt sich zwar mit geeigneten Provisionierungs/Managementsystemen wie z. B. dem Cisco-propietären Group-Encrypted-Transport-VPN (getVPN) drücken. Ein IPsec-VPN sollte aber erst zusätzlich zum Einsatz kommen, wenn selbst die Kombination aus TLS/SRTP und MPLS-VPN speziellen Compliance-Vorgaben nicht mehr gerecht wird.

| | Schutzbedarf * | | |
|---|---|---|---|
| SIP-Trunk/IP-Anbindung | Normal | Hoch | Sehr hoch |
| Fremd-Internetanschluss | mit TLS/SRTP und Firewall/E-SBC-Schutz | nicht empfehlenswert | nicht empfehlenswert |
| Internet/Dual-Play-Anschluss des ITSP, ohne Voice-Port | mit Firewall/E-SBC-Schutz | mit TLS/SRTP und Firewall/E-SBC-Schutz | nicht empfehlenswert |
| Internet/Dual-Play-Anschluss des ITSP mit Voice-Port (gemäß Bild 3) | so nutzbar | mit TLS/SRTP und E-SBC-Schutz | nicht empfehlenswert |
| Voice-only/Single-Play-Anschluss des ITSP (gemäß Bild 2) | so nutzbar | mit TLS/SRTP und E-SBC-Schutz | mit TLS/SRTP und E-SBC-Schutz |
| MPLS-IP-VPN-Anbindung des ITSP | so nutzbar | mit E-SBC-Schutz | mit TLS/SRTP und E-SBC-Schutz. |

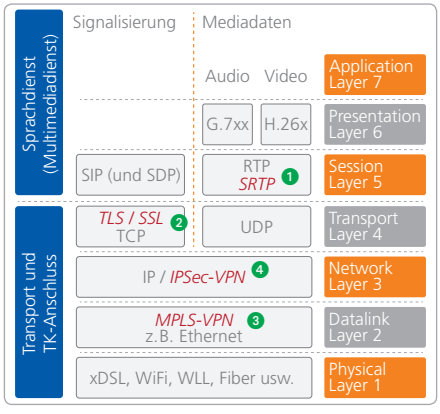
** Schutzbedarfskategorie gemäß BSI-Grundschutz*

**Tabelle 1:** Empfehlungen für Sicherungsmaßnahmen

Bleibt die Frage, wann welches Sicherungsprotokoll genutzt werden sollte. Die Antwort hängt vor allem von diesen beiden kundenindividuellen Vorgaben ab: Wie sieht die Netztopologie für die komplette Übertragungsstrecke des SIP-Trunks aus und in welche Schutzbedarfskategorie (normal, hoch, sehr hoch) will sich der Kunde eingereiht sehen? Basierend auf diesen Angaben empfiehlt der Autor die in **Tabelle 1** genannten Sicherungsmaßnahmen.

## Schlussbemerkung

Der Gedanke, Internet-Telefonie sei unsicherer als ISDN-Telefonie, lässt sicher noch einige Kunden so lange wie möglich auf ihrem bisherigen ISDN-Sprachanschluss beharren. Schaut man sich SIP-Trunking jedoch im Detail an, sieht man u. a., dass die Sprache hier ja meist gar nicht durch das offene Internet zum Kunden kommt, sondern über IP-Verbindungen, die vom Internet abgeschottet sind. Auch konnten die Daten eines ISDN-Anschlusses nicht verschlüsselt werden – die eines SIP-Trunks jedoch schon. Und auch bezüglich der Diensteverfügbarkeit beim Kunden kann beim SIP-Trunking eine Zuführungs- und Plattformredundanz geschaffen werden, wie sie bei ISDN nicht möglich war. Aus der Sicht des Autors sollte sich jetzt jeder Anwender für einen in absehbarer Zeit anstehenden Wechsel in der Anschlusstechnologie beispielsweise durch sein betreuendes TK-Fachunternehmen kundig beraten lassen. Die Topologie des Kommunikationsnetzwerks muss aufgenommen und der Schutzbedarf des Kunden ermittelt werden beziehungsweise geklärt sein. Daraufhin können die individuell passenden Empfehlungen ausgesprochen werden. ■




Grafik: VAF/QSC

**Bild 4:** In vier Layern des ISO/OSI-Schichtenmodells können Sicherheitsprotokolle für die Kommunikationssicherheit des SIP-Trunks genutzt werden.

Quellen:
***[BSI01]:*** *Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge, Maßnahmen zur Organisation. www.bsi.bund.de*

Autor:

**Dipl.-Ing. Andreas Steinkopf** ist Produktmanager für VoIP bei der Kölner QSC AG, die eines der größten deutschen NGNs betreibt und u. a. SIP-Trunks, Internet- und IP-VPN-Anschlüsse im indirekten Kanal vermarktet. **www.qsc.de**