LANCOM Whitepaper
Session Border Controller

Neue Sicherheitsanforderungen durch All-IP

Mit der Überführung ehemaliger ISDN- in All-IP-Anschlüsse reihen sich multimediale und zugehörige Signalisierungsdaten neben dem generellen Datenverkehr in die Riege IP-basierter Anwendungen ein. Dies bringt diverse Anforderungen an die Netzwerkinfrastruktur mit sich: Neben einem VoIP-fähigen Router, der den Annex-J-Standard unterstützt, und dem Vorhandensein geeigneter Quality-of-Service-Mechanismen, sollte zwingend auch die Netzwerksicherheit überprüft werden. Zur Absicherung von IP-Netzwerken ist dabei eine Firewall – integriert in den Router oder als separate Netzwerkkomponente – essentiell. Diese schützt das Netzwerk vor unbefugtem Zugriff, überwacht den durchlaufenden Verkehr und entscheidet regelbasierend, ob bestimmte Datenpakete durchgelassen werden.

Allerdings sind Firewalls nicht in der Lage, mit SIP-basierten Sprachpaketen (Voice over IP) geeignet umzugehen, da diese die benutzten Ports dynamisch aushandeln und in der Payload übermitteln. Einfach alle Ports für VoIP und Multimedia-Anwendungen „per se" zu öffnen ist keine gute Idee, wenn man bedenkt, dass alle VoIP-Endgeräte als mit der Außenwelt verbundene „Mini-Rechner" vollständigen Zugang zum Firmennetz bieten, oder aber – entsprechend manipuliert – leicht zum Abhören oder Mitschneiden von Gesprächen, beispielsweise durch ein von außen gesteuertes Aktivieren der Mikrofone missbraucht werden können.

Um dieser potenziellen Schwachstelle entgegenzuwirken, ist eine sichere Trennung des (unsicheren) externen Netzes vom (sicheren) internen Netz zu gewährleisten. Genau diese Aufgabe erfüllt ein Session Border Controller.

Funktionsweise

Wie der Name „Session Border Controller" (SBC) impliziert, kontrolliert er an der Netzwerkgrenze („Border") den Auf- und Abbau sogenannter Sitzungen („Sessions") (Abb. 1).

Anders als eine Firewall ist ein SBC in der Lage, an der Netzwerkgrenze Echtzeit-SIP-Kommunikation im Bereich der Signalisierungsdaten (Control Plane) und der Sprach- bzw. Mediadaten (Data Plane) zu untersuchen, zu kontrollieren und zu steuern. Er steuert den Aufbau, die Durchführung und den Abbau von Telefonaten und die dazugehörigen Datenströme bezüglich Signalisierung und Mediendaten wie Sprache oder Video.

Als Proxy für SIP-Kommunikation terminiert ein SBC zunächst jede Session, also beispielsweise einen extern eingehenden Anruf, und setzt anschließend eine neue Session für das interne Gespräch auf. Bei diesem Vorgang werden Signalisierungsdaten und Media Streams untersucht, validiert und ggf. transformiert. Dabei kommen die Vorteile eines SBCs in den Bereichen Sicherheit und Qualität zum Tragen:

Abb. 1: Funktionsweise eines Session Border Controllers

LANCOM Systems

Sicherheit

Im SBC eingehende und ausgehende Sessions werden terminiert und auf Layer-5-Ebene (SIP) überprüft. Nur bekannte und unterstütze Steuerungsbefehle werden weitergeleitet. Dabei bietet der SBC als Applikations-Firewall Zugangsschutz für Sprache, Video und Multimedia. Er überwacht erlaubte Sessions und versteckt ihren topologischen Ursprung, wie beispielsweise interne IP-Adressen von Servern und Telefonen. Darüber hinaus schützt der SBC die Vertraulichkeit von Echtzeit-Sprachdaten gegen Abhören, Mitschneiden und Man-in-the-Middle-Attacken durch die optionale Verschlüsselung und über Prüfsummen (Secure Real-Time Transport Protocol, SRTP), sofern die Gegenstelle – beispielsweise ein SBC auf Providerseite – die so verschlüsselten SIP-Pakete wieder entschlüsseln kann. Ebenso werden ausgehende Signalisierungsdaten über TLS verschlüsselt (Session Initiation Protocol Secure, SIPS) und bei Eingang entsprechend entschlüsselt.

Qualität

SIP ist, obwohl IP-basierend, kein einheitliches Kommunikationsprotokoll: Hersteller und Provider implementieren den SIP-Standard in der Praxis so unterschiedlich – beispielsweise über proprietäre Header in SIP-Paketen –, dass im schlimmsten Fall seitens der TK-Anlage eine eingehende Session mit ihr unbekannten Parametern als Angriff interpretiert und verworfen wird. Ein Session Border Controller erkennt jegliche Arten an SIP-Headern und „normalisiert" diese für die dahinterliegende TK-Anlage, um eine hersteller- und providerübergreifende Interoperabilität zu gewährleisten.

Ein ähnlicher Fall liegt in den verschiedenen eingesetzten bzw. unterstützten Codecs der TK-Gegenstellen. Ein SBC erkennt, welche Codecs die beteiligten TK-Anlagen unterstützen, ob es gemeinsame Codecs gibt oder ob eine Konvertierung in einen gemeinsam nutzbaren Codec (Transcoding) notwendig ist. Sind die beiden beteiligten TK-Gegenstellen beispielsweise eine moderne HD-Voice-fähige TK-Anlage und eine ältere ISDN-Anlage, ist eine Umwandlung von HD-Voice auf den G.711-Codec notwendig. Dabei übernimmt der SBC diese Mediation und wählt den effizientesten Kommunikationsweg bzw. den auf beiden Seiten verfügbaren und idealen Codec für die jeweilige Session.

Im Bereich Faxübertragung in gemischten Umgebungen mit einer IP- und einer ISDN-Gegenstelle kann z.B. ein SBC erkennen, ob die Gegenstelle das IP-basierte Faxprotokoll T.38 unterstützt oder nicht. Falls nicht, wandelt er das Fax-Paket in das ISDN-basierte T.30 um (Transcoding), damit die Faxübertragung reibungslos funktioniert.

Darüber hinaus reserviert der SBC die für VoIP-Telefonate benötigte Internetbandbreite (Quality of Service), um eine hohe Gesprächsqualität zu gewährleisten. Notrufe werden als solche erkannt und gegenüber anderen Telefonie-Sitzungen priorisiert.

Zusammenarbeit mit dem Voice Call Manager (VCM)

Der SBC arbeitet in der Praxis eng mit einer weiteren Komponente für VoIP zusammen: dem Voice Call Manager. Dieses bezeichnet die Komponente, die für TK-Anlagenfunktionen, Endgeräte-Verwaltung, Rufnummernzuordnung und -manipulation sowie die Call-Routing-Tabelle zuständig ist.

Diese Rolle übernimmt klassisch eine TK-Anlage, mit der zentralen Aufgabe, einen zur Vermittlung anliegenden Ruf einer bestimmten Leitung oder einem bestimmten Endgerät zuzuordnen. Dabei werden die gewählten Rufnummern manipuliert, aufgelöst und den in einer Call-Routing-Tabelle definierten Regeln entsprechend an den gerufenen Teilnehmer weitergeleitet. Auch während eines Gesprächs kann ein Ruf über Befehle wie halten, makeln oder verbinden manipuliert und weitergeleitet werden. Gerade für kleinere TK-Szenarien sparen diese Call-Management-Funktionen häufig den Betrieb einer separaten TK-Anlage.

Session Border Controller im Einsatz

Grundsätzlich wird ein Session Border Controller als Schnittstelle zwischen Router / Firewall und der internen Telefonie-Infrastruktur eingesetzt. Dabei handelt es sich im Unternehmensumfeld meist um eine zentrale TK-Anlage. Zunehmend wird aber auch auf eine externe TK-Anlage aus der Cloud gesetzt, die das Telefonie-Management übernimmt. Die folgende Darstellung (Abb. 2) zeigt eine Netzwerktopologie, in der Firewall, SBC, Router und TK-Anlage als separate Komponenten eingesetzt werden.

Eine elegantere – und schlankere – Lösung (Abb. 3) besteht aus einem hochintegrierten Business-Router, der die Funktionen einer Firewall und eines Session Border Controllers beinhaltet. Dabei steht der Router als erstes Gerät am Netz und übernimmt die gesamte Verwaltung des Datenverkehrs und die Umsetzung der Firewall-Regeln. Er dient als SIP-Gateway zwischen TK-Anlage und All-IP-Netz und übernimmt als Session Border Controller die sichere Trennung von internem und externem Netzwerk sowie das QoS-Management.

Abbildung 4 zeigt die vollständige Integration aller Funktionen in einem einzigen Router, bei dem zusätzlich der VCM die zentralen Funktionen einer TK-Anlage abbildet. Dieses Szenario eignet sich daher besonders gut für kleinere Unternehmen.

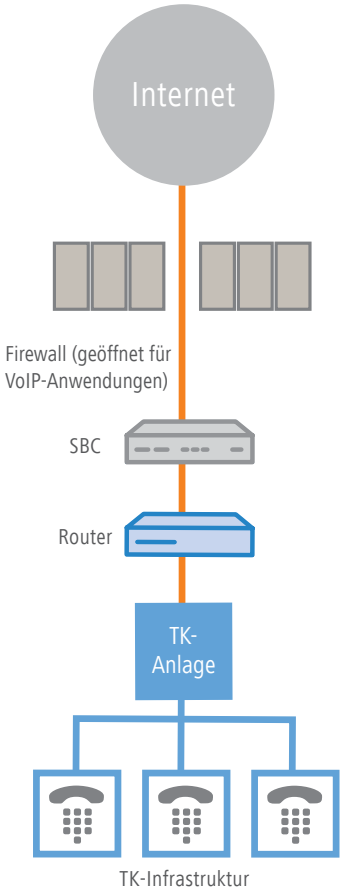

Abb. 2: Netzwerktopologie mit separaten Komponenten für mittlere und große Netzwerke

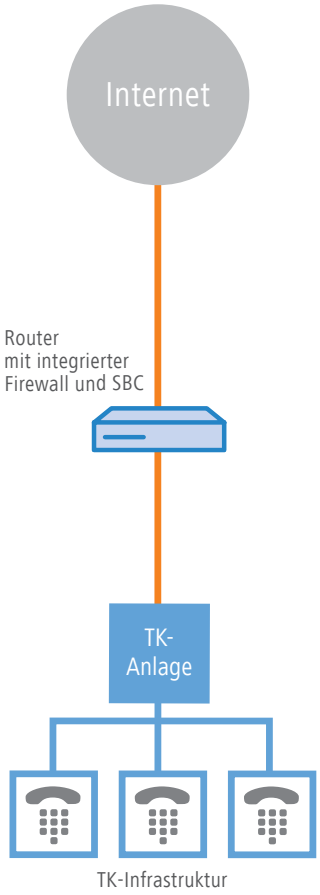

Abb. 3: Router mit integrierter Firewall und SBC für mittlere und große Netzwerke

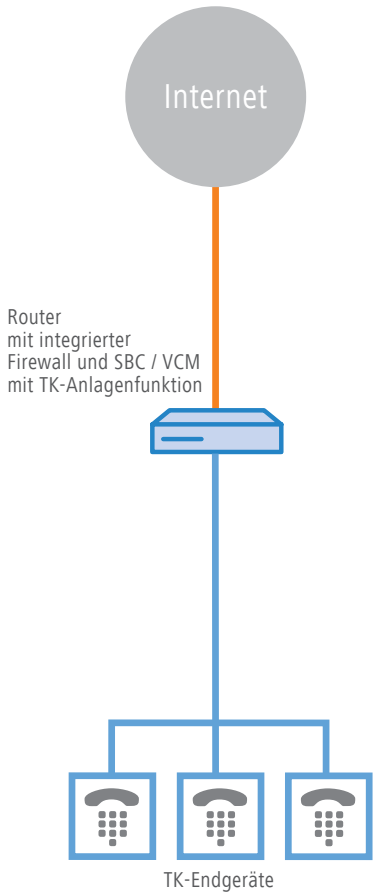

Abb. 4: Router mit integrierter Firewall und SBC / VCM mit TK-Anlagenfunktion für kleine Netzwerke

LANCOM Systems

Eindeutige BSI-Empfehlung

Das Bundesamt für Sicherheit in der Informationstechnik gibt eine klare Einsatzempfehlung für die oben beschriebene „schlanke" Lösung: In der **Technischen Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf** (Stand August 2014) wird zum Thema **M-TK-47 Verwendung eines Session Border Controller zur Absicherung eines IP-Anlagenanschlusses** für Unternehmen der generelle Einsatz eines SBCs als Peripheriegerät zwischen WAN-Anschluss und interner TK-Anlage bzw. Provider empfohlen. Darüber hinaus gilt folgende Erläuterung bzw. Einschränkung für kleinere Organisationen und kleinere Standorte: „Insbesondere für kleinere Standorte können auch Kombigeräte eingesetzt werden, welche zugleich Firewall, SBC und Internet- bzw. WAN-Anbindung übernehmen können. Hierbei ist das Thema Verfügbarkeit angemessen zu berücksichtigen."

(Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeLeitlinien/TKAnlagen/TLSTK_II-Teil_2%E2%80%93Sicherheitskonzepte.pdf?__blob=publicationFile&v=1)

Fazit

Ein Session Border Controller ist ein elementarer Bestandteil sicherer und zuverlässiger Telefonie im Geschäftsumfeld, weil er speziell im Kontext VoIP für eine sichere Trennung des privaten Netzes und der Außenwelt sorgt. Der Einsatz eines passenden SBC sollte bei der Netzwerkplanung zwingend berücksichtigt werden. Kombinierte Geräte vereinen mittlerweile die Funktionen von Router, Voice Call Manager, Firewall und SBC in einem Gerät und minimieren so Anschaffungs-, Einrichtungs-, Betriebs- und Wartungsaufwände.

Insbesondere in Unternehmen mit sensibler Datenkommunikation und komplexer Telefonie-Infrastruktur ist ein Session Border Controller somit Kernelement in den Bereichen Sicherheit und zuverlässige Telefonie.