



Cyberangriffe über VoIP? Wie können Sie Ihre Telefonie schützen?



Welche Maßnahmen sollten Sie als Unternehmer ergreifen, um Ihre Telefonie – und damit auch ihre Daten – zu sichern? Ein Patentrezept gibt es auch hier nicht. Denn jeder Unternehmer muss individuell bewerten, welches Niveau die VoIP-Sicherheit braucht. Grundsätzlich gibt es aber zumindest zwei wichtige Bestandteile: den Einsatz von Session Border Controllern (SBC, VoIP-Firewall) und den Verschlüsselungsbedarf. Wir zeigen Ihnen wie ein SBC funktioniert und wie Sie ihn in Ihrem Unternehmen einsetzen können.

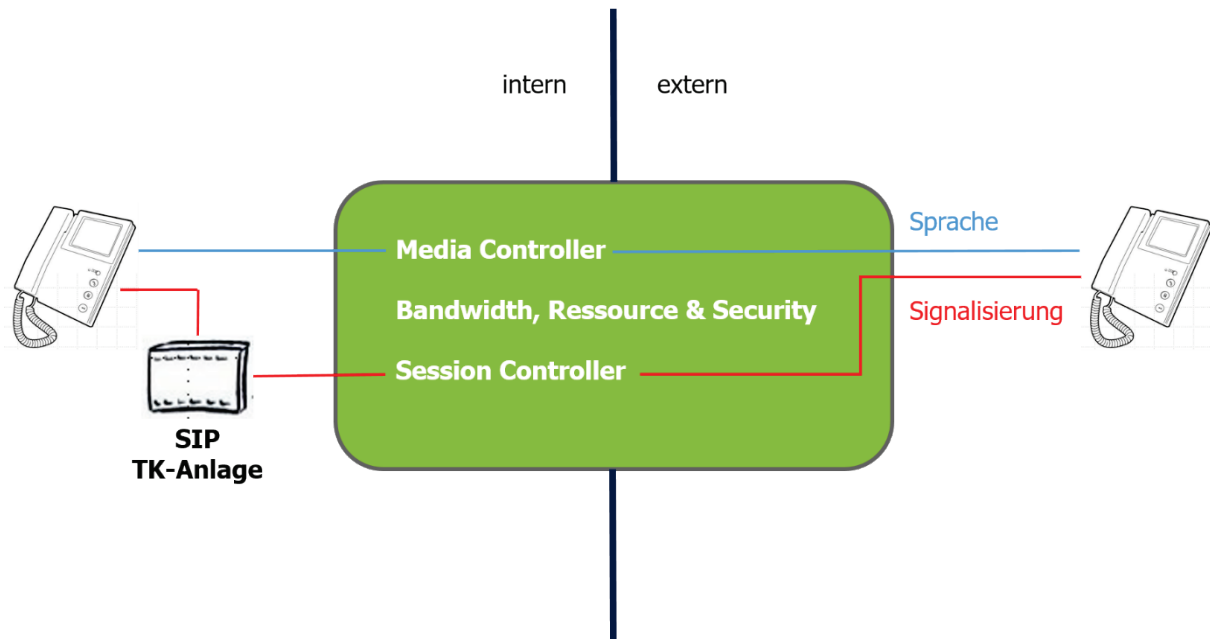
Was ist ein Session Border Controller (SBC)?

Ein Session Border Controller (SBC) ist eine Netzwerkkomponente, die Sitzungen zwischen internen und externen Datennetzen herstellt. Bei der IP-Telefonie soll der SBC für eine sichere Kommunikation sorgen.

Die Funktion eines „Session Border Controllers“ (SBC) erschließt sich aus den drei Bestandteilen des Begriffs: Session (Sitzung), Border (Grenze) und Controller (Kontrolleinheit). Immer dann, wenn verschiedene Rechnernetze miteinander verknüpft werden, besteht die Gefahr von Sicherheitslücken. Der Controller minimiert die Risiken, indem er die Einhaltung von Zugriffsrechten gewährleistet und so eine Kommunikation unter hohen Sicherheitsstandards ermöglicht.

In technologischer Hinsicht handelt es sich bei einem SBC um ein Netzwerkgerät, das im Markt sowohl als Hardware-Appliance als auch als reine Software-Komponente angeboten wird. Das Hauptanwendungsgebiet ist die IP-Telefonie. Bei VoIP (Voice over IP) wird über Datennetze und das Session Initiation Protocol (SIP) telefoniert. Wenn die Netze der Gesprächsteilnehmer miteinander in Kontakt treten, muss dafür gesorgt werden, dass nur ordnungsgemäße SIP-Nachrichten übertragen werden.

An der Stelle kommt der SBC ins Spiel, indem er für die Session, also die Telefonsitzung, als eine Art Firewall fungiert. Dabei stellt er sicher, dass das interne Netzwerk eines Unternehmens durch einen externen Anrufer keine Bedrohung erfährt. In der Regel besteht ein Controller aus drei technologischen Elementen: einer Einheit, die die Sprachverbindung aufbaut und am Laufen hält, einer zweiten, die die Signale überwacht, und einer dritten, die die notwendige Bandbreite zur Verfügung stellt und für die Datensicherheit sorgt.



Unterschied zur Firewall

Die Spezialisierung macht den Unterschied, wenn man einen SBC mit anderen Geräten für die Netzwerksicherheit vergleicht. So schützt eine klassische Firewall ein Netzwerk im Hinblick auf den Datenverkehr, der in einem Unternehmen stattfindet, während der SBC die IP-Telefonie absichert. Bei Gesprächen ist er oft die erste Schutzvorrichtung, die noch vor anderen Mechanismen greift.

Die Bedeutung von SBCs dürfte weiter zunehmen. Der Grund dafür liegt darin, dass die IP-Telefonie kontinuierlich auf dem Vormarsch ist und die klassische ISDN-Technologie ablöst. Weil Sprache und Daten bei VoIP über dasselbe Netz übertragen werden, ist die Sicherheit der Telefonie ein zentrales Element der Sicherheit des gesamten Netzwerks. Ein SBC ist in diesem Zusammenhang die geeignete Komponente, mit der sich die Sprachkommunikation schützen lässt.

Fazit

Wie immer ist es von enormer Bedeutung die Umstellung auf IP-Telefonie gut zu planen. Cyberattacken können auch Ihr Unternehmen betreffen.

Lassen Sie sich am besten von Profis beraten, um ein sicheres Konzept für Ihr Unternehmen zu planen. Es geht um die Sicherheit Ihrer Daten!

**1 Stunde gratis ALL-IP
Strategie-Beratung**

<https://www.gfk-system.de/home/strategieberatung>

Bitte klicken Sie hier, um
einen Termin mit unserem
IP-Strategieprofi zu
vereinbaren.

