Sicherheitsleitfaden
für VoIP-Telefonie

ansit com
Business Communication that rocks.

Einleitung

Voice-over-IP (VoIP) ist heute in vielen Unternehmen Standard. Kein Wunder, denn die Technologie bringt jede Menge Vorteile mit sich. Doch wie bei allen internet-basierten Systemen gibt es auch bei der VoIP-Telefonie gewisse Risiken. Deshalb ist es uns wichtig, Sie für mögliche Sicherheitslücken zu sensibilisieren und Ihnen zu zeigen, wie Sie sich bestmöglich davor schützen können.

Unsere Empfehlung: Setzen Sie möglichst alle sinnvollen Sicherheitsmaßnahmen konsequent um und holen Sie bei Bedarf Ihre IT-Abteilung oder einen IT-Dienstleister mit ins Boot. Bei Fragen rund um Datenschutz, Sicherheit oder VoIP-Telefonie sind wir natürlich gern für Sie da.

ansitel Telefonanlagen sind bereits mit zahlreichen Sicherungssystemen ausgestattet, die eine Vielzahl unterschiedlicher Bedrohungsszenarien abwenden können. Um die Sicherheit zu erhöhen, ist jedoch auch die Absicherung anderer Netzwerkgeräte sowie die Sensibilisierung Ihrer Mitarbeitenden wichtig.

Im hinteren Teil dieses Sicherheitsleitfadens für VoIP-Telefonie finden Sie eine Checkliste, die Ihnen die wichtigsten Maßnahmen noch einmal zusammenfassend aufzeigt. Bitte beachten Sie, dass dieser Sicherheitsleitfaden immer eine Momentaufnahme ist und nicht alle Bedrohungsszenarien und Maßnahmen umfassen kann. Wir empfehlen Ihnen daher, immer die News des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu beachten.

Häufige Bedrohungen und Gefahren

Abhören bzw. Mithören von Gesprächen

Telefonate via Voice over IP werden über das Internet übetragen. Das bringt viele Vorteile, birgt aber auch Risiken. Wenn veraltete Firmware (z.B. von IP-Telefonen, Telefonanlagen, Netzwerkgeräten), unsichere Standardprotokolle oder fehlerhaft konfigurierte Netzwerkkomponenten im Spiel sind, kann es passieren, dass Sprachpakete abgefangen und rekonstruiert werden. Das Ergebnis: Unbefugte könnten Gespräche oder Teile davon mithören, ohne dass Sie es bemerken.

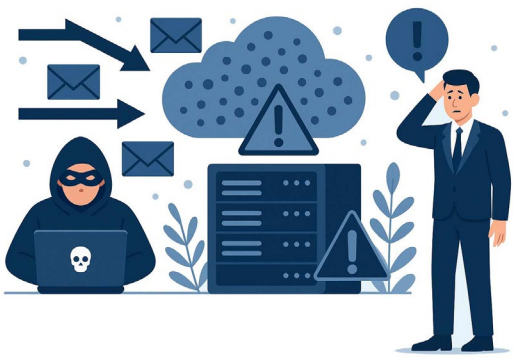
Telefonanlagen-Hacking

Die Telefonanlage ist das Herzstück Ihrer Geschäftskommunikation. Moderne VoIP-Anlagen lassen sich bequem über eine Weboberfläche konfigurieren und verwalten. Doch genau hier lauert eine Gefahr: Wenn der Computer, mit dem auf diese Oberfläche zugegriffen wird, mit Schadsoftware (z. B. Viren oder Trojanern) infiziert ist, können Angreifer Zugriff auf das gesamte Telefonsystem erlangen.

Auch schwache oder unsichere Passwörter sind ein Einfallstor. Gerät eine Anlage in falsche Hände, können Kriminelle kostenintensive Auslandsgespräche führen, Endgeräte manipulieren oder Verbindungen umleiten. Das passiert in der Regel zunächst unbemerkt und kann sehr teuer werden.

DoS-Attacke – Wenn nichts mehr geht

DoS steht für **Denial of Service** – also der Angriff auf die Verfügbarkeit eines Dienstes. Dabei wird ein Server oder Netzwerk gezielt mit einer Flut an Daten überlastet, bis er nicht mehr erreichbar ist. Erfolgt der Angriff nicht nur von einem einzelnen Rechner, sondern über ein ganzes Netzwerk kompromittierter Geräte, spricht man von einer DDoS-Attacke (Distributed Denial of Service).



Im Bereich der VoIP-Telefonie sind vor allem Cloud-Telefonanlagen und die Server von Telefonieanbietern gefährdet. Kommt es zu einer solchen Überlastung, kann dies dazu führen, dass eingehende und ausgehende Anrufe nicht mehr möglich sind – was in Unternehmen schnell zu ernsthaften Störungen führt.

Diebstahl von SIP-Zugangsdaten – ein teures Risiko

Wer Zugriff auf Ihre SIP-Zugangsdaten hat, kontrolliert im Grunde Ihren Telefonanschluss, so, als hätte jemand Ihren Haustürschlüssel kopiert. Kriminelle können damit kostenpflichtige Auslandsgespräche führen, interne Kommunikation ausspionieren oder Ihre Rufnummer missbrauchen.

Derartige Datenverluste passieren oft durch Phishing-E-Mails, unsichere Passwörter, ungenügend geschützte Endgeräte oder schlecht gesicherte Telefonanlagen, die aus dem Internet erreichbar sind. Auch Passwörter, die nie geändert wurden oder mehrfach verwendet werden, sind ein gefundenes Fressen für Angreifer.

Einmal in falschen Händen, entstehen oft **innerhalb weniger Stunden hohe Kosten**, meist durch Anrufe in Premium-Zielregionen (z. B. Karibik oder Afrika), die automatisiert im großen Stil erfolgen.

Man-in-the-Middle – Mitlauschen im Schatten

In schlecht gesicherten Netzwerken, etwa öffentlichen WLANs oder unsauber konfigurierten Firmen-VPNs, können Angreifer sich zwischen Ihr Telefon und dem SIP-Server schalten. Dabei „hören“ sie mit, ohne entdeckt zu werden. Dieses Szenario nennt man Man-in-the-Middle (MitM).

Sind SIP- oder Sprachverbindungen unverschlüsselt, können Gesprächsdaten und Zugangsdaten abgefangen oder sogar manipuliert werden. Besonders kritisch: Der Angriff ist für Nutzer in der Regel nicht erkennbar.

Voicemail- und IVR-Hacking – Angriffe durch die Nebenstelle

Voicemail-Systeme oder Sprachmenüs (IVR = Interactive Voice Response) sind praktisch, aber oft unzureichend abgesichert. Angreifer versuchen hier, mit Standard-PINs oder durch automatisiertes Durchprobieren Zugriff zu bekommen.

Einmal eingeloggt, können sie Sprachnachrichten abhören, interne Informationen abfragen oder sogar Funktionen missbrauchen und damit z. B. teure Rückrufe auslösen oder Durchwahlen manipulieren.

Missbrauch offener SIP-Ports – Einladung für Bots

Viele IP-Telefonanlagen und Endgeräte sind standardmäßig über das Internet erreichbar, meist über offene SIP-Ports (z. B. Port 5060). Das Problem: Diese Schnittstellen werden regelmäßig automatisiert gescannt und attackiert.

Angreifer versuchen mit sogenannten **SIP-Scan-Bots**, Zugangsdaten zu erraten, Systeminformationen auszulesen oder sogar direkte Anrufe zu platzieren – oft ohne dass Administratoren es sofort bemerken.

Rufnummern-Spoofing - Täuschung mit Ihrer Nummer

Beim sogenannten Caller ID Spoofing fälschen Angreifer gezielt die Absendernummer eines Anrufs. Das Ziel: Vertrauen schaffen und Mitarbeitende täuschen, etwa durch angeblich interne Rufnummern, Behörden oder Dienstleister.

Solche gefälschten Anrufe werden oft im Rahmen von Phishing oder CEO-Fraud eingesetzt. In vielen Fällen wird sogar Ihre eigene Nummer als Absender genutzt, was zu Rückfragen oder Missbrauch führen kann.

Sicherheitsmaßnahmen

Sichere Passwörter und Passwortzugänge

Verwenden Sie grundsätzlich **starke und komplexe Passwörter**. Ein sicheres Passwort besteht idealerweise aus einer Kombination von **Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen** und ist dabei möglichst lang. Denn: Je länger ein Passwort, desto aufwändiger ist es zu knacken – selbst mit automatisierten Angriffen.

Speichern Sie Passwörter **nicht im Browser** und geben Sie sie nur weiter, wenn es absolut notwendig ist. Nutzen Sie stattdessen einen professionellen **Passwort-Manager**, wie z. B. KeePass oder Passbolt, um Ihre Zugangsdaten sicher zu verwalten. So behalten Sie den Überblick und reduzieren das Risiko von Datenmissbrauch.

In diesem Zusammenhang ist es auch wichtig zu erwähnen, dass sämtliche Mitarbeiter und Mitarbeiterinnen im Unternehmen sensibilisiert werden.

Regelmäßiges Ändern von Passwörtern

Es ist empfehlenswert, Passwörter in regelmäßigen Abständen zu ändern, idealerweise alle sechs Monate. So wird das Risiko verringert, dass langfristig kompromittierte Zugangsdaten unbemerkt ausgenutzt werden.

Unabhängig vom Zeitintervall gilt: Immer dann, **wenn sich Verantwortlichkeiten ändern**, etwa bei einem neuen Administrator oder dem Ausscheiden eines Technikers, sollten sämtliche betroffenen Passwörter umgehend aktualisiert werden. Nur so bleibt der Zugriff kontrollierbar und nachvollziehbar.

Updates und Instandhaltung der Systeme

Telefone und Telefonanlagen werden im Laufe ihrer Produktlebensdauer kontinuierlich weiterentwickelt, auch und gerade im Hinblick auf Sicherheitsfunktionen und Systemstabilität. Dazu zählen regelmäßige Sicherheitsupdates (Security-Patches), die bekannte Schwachstellen beheben.

Stellen Sie deshalb sicher, dass **alle Komponenten Ihrer Infrastruktur**, also Router, Firewalls, TK-Anlagen, Endgeräte und Betriebssysteme, **stets auf dem aktuellen Stand** sind. Nur so kann gewährleistet werden, dass Ihre Systeme gegen bekannte Bedrohungen geschützt bleiben.

Firewall

Eine Firewall ist ein zentrales Sicherheitsinstrument, das einzelne Geräte (z. B. Ihre TK-Anlage), ganze Netzwerke oder Server vor unbefugten Zugriffen schützt, insbesondere aus dem Internet. Firewalls können sowohl hardwarebasiert (z. B. als dediziertes Gerät) als auch softwarebasiert (z. B. direkt auf einem Server) implementiert werden.

Wir empfehlen den grundsätzlichen Einsatz von Firewalls, um Ihre Kommunikationsinfrastruktur zuverlässig gegen externe Angriffe abzusichern.

Tipp: Öffnen Sie in der Firewall nur die unbedingt erforderlichen IP-Adressen und Ports Ihres Providers. Vermeiden Sie, wenn möglich, Portweiterleitungen (Port Forwarding) und sperren Sie ungenutzte Subnetze konsequent. Weniger ist hier mehr – jede unnötige Öffnung ist ein potenzielles Einfallstor.

Sicherheitsfunktionen bei Telefonieprovidern

Viele VoIP-Provider bieten hilfreiche Sicherheitsmechanismen zur Kostenkontrolle an, zum Beispiel durch die Möglichkeit, Tages- oder Monatslimits für Anrufkosten festzulegen. Wenn Sie Ihr typisches Anrufvolumen einschätzen können, empfiehlt es sich, ein festes Tageslimit zu setzen. Sollte ein Angreifer Zugriff auf Ihren Account erlangen, bleibt der finanzielle Schaden dadurch begrenzt.

Darüber hinaus erlauben einige Anbieter das gezielte Sperren von Ländern oder Ländervorwahlen, um unerwünschte Auslandsgespräche proaktiv zu unterbinden.

Wichtig: Behalten Sie immer die Hoheit über Ihre Zugangsdaten. Geben Sie weder Benutzername noch Passwort in fremden Korrespondenzen oder unsicheren Umgebungen weiter.

Wenn Sie eine ansitel Telefonanlage nutzen, sind teure Zonen standardmäßig deaktiviert. Über die Option „Teure Zonen aktivieren“ können exakt die Länder ausgewählt werden, in dem Auslandstelefonie erlaubt sein soll.

Verschlüsselung nutzen, wo immer möglich

Sowohl der Zugriff auf Ihre Telefonanlage per Webbrowser als auch der eigentliche Telefonanschluss lassen sich in vielen Fällen verschlüsseln, und sollten es auch.

Beispielsweise können sich viele VoIP-Telefone prinzipiell an beliebigen SIP-Anlagen anmelden. Um das zu verhindern, sollte die Anmeldung auf eine definierte Telefonanlage beschränkt werden, etwa durch eine Kombination aus starkem Passwortschutz und der Zuweisung fester IP-Adressen im Endgerät.

Die meisten SIP-Provider unterstützen heute TLS (Transport Layer Security) zur Verschlüsselung der Signalisierungsdaten – also der Informationen über Rufnummern, Gesprächsaufbau usw. Zusätzlich bieten viele Anbieter SRTP (Secure Real-Time Transport Protocol) an, um Audio- und Videodaten verschlüsselt zu übertragen. SRTP wurde speziell für VoIP-Kommunikation entwickelt und schützt zuverlässig vor dem Mithören.

Regelmäßige Backups

Erstellen Sie in regelmäßigen Abständen Backups Ihrer Systeme, insbesondere der Konfiguration Ihrer Telefonanlage. Im Falle eines Ausfalls, eines Angriffs oder einer fehlerhaften Änderung kann so eine funktionsfähige Version schnell wiederhergestellt werden.

Achten Sie darauf, dass Ihre Backups nicht auf dem gleichen Gerät oder Netzwerkspeicher abgelegt werden wie die produktiven Systeme. Externe Speicherorte oder automatisierte Cloud-Backups erhöhen die Ausfallsicherheit und schützen vor Datenverlust, z.B. bei Hardwaredefekten oder Ransomware-Angriffen.

Monitoring und Anomalie-Erkennung

Moderne Telefonanlagen und Provider bieten Funktionen zur Überwachung des Verbindungsverhaltens. Auffällige Aktivitäten, z. B. viele Anrufversuche in kurzer Zeit oder zu ungewöhnlichen Zeiten, hohe Auslastung des Arbeitsspeichers der Telefonanlage, plötzlich nicht mehr verfügbare Leitungen, abgemeldete Telefone, können so frühzeitig erkannt und auf ein mögliches Schadrisiko ausgewertet werden.

ansitel Telefonanlagen unterstützen direkt das Monitoring der Telefonanlage. Hierzu empfehlen wir das Monitoringtool Zabbix.

Endgeräte absichern

Auch Telefone selbst sind potenzielle Angriffspunkte, besonders, wenn sie direkt mit dem Internet verbunden sind oder Standardzugänge nicht geändert wurden.

Tipp: Sichern Sie Admin-Zugänge mit starken Passwörtern ab, deaktivieren Sie nicht benötigte Dienste auf Endgeräten und halten Sie, wenn möglich, die Firmware der Geräte immer auf den aktuellsten Stand.

Spezialfall: Social Hacking und Social Engineering

Social Engineering bezeichnet den Versuch, Menschen durch gezielte Täuschung zu Handlungen zu verleiten, die sicherheitskritisch sind, z. B. die Herausgabe von Zugangsdaten oder das Ausführen bestimmter Konfigurationen.

Typische Anzeichen für Social-Hacking-Versuche:

- Unerwartete Anrufe mit „technischen Problemen“ oder „Sicherheitswarnungen“
- Aufforderungen zur Weitergabe von Passwörtern oder anderen Zugangsdaten
- Absetzen von Phishing-Mails, die z.B. Provider täuschend echt nachah-mmen und oft auffordern, ein Passwort zurückzusetzen
- Dringlichkeit, Druck oder angeblicher Handlungszwang („sofort nötig“, „Chef verlangt das“)

Was Sie tun können:

- Geben Sie niemals Passwärter oder Zugangsdaten telefonisch oder per Mail weiter.
- Bestätigen Sie Rückfragen bei sensiblen Vorgängen immer über einen zweiten, offiziellen Kanal
- Prüfen Sie die Links von Buttons in Emails sowie die echte Absenderadresse
- Schulen Sie Mitarbeitende regelmäßig für typische Täuschungs-versuche im Arbeitskontext

Session Border Controller (SBC) als Sicherheitsinstanz

Ein Session Border Controller (SBC) übernimmt die sichere Vermittlung und Überwachung von SIP-Verbindungen zwischen Ihrer Telefonanlage und dem VoIP-Provider (Telefonanschluss). Er schützt Ihre Infrastruktur vor Angriffen, kontrolliert den Zugriff und sorgt für die technische Kompatibilität.

Typische Funktionen eines SBC:

- Blockieren unerwünschter SIP-Anfragen
- Schutz vor Port-Scanning und DoS-Attacken
- Verschlüsselung und Transkodierung von Sprachdaten
- Netzwerksegmentierung und IP-Adressenmaskierung

Tipp: Der Einsatz eines SBC ist besonders sinnvoll bei Cloud-Telefonanlagen, öffentlichen SIP-Trunks, bei der Verwendung von SIP-Clients oder verteilten Standorten.

Security-Checkliste für Ihre Kommunikationsinfrastruktur

Basis-Schutz (schnell umsetzbare Maßnahmen)

- ☐ Starke, individuelle Passwörter für Weboberflächen und VoIP-Zugänge vergeben
- ☐ Passwörter regelmäßig ändern (alle 6 Monate oder bei Personalwechsel)
- ☐ Vergewissern Sie sich, dass Passwörter nicht im Browser gespeichert sind
- ☐ Backup der Telefonanlagen-Konfiguration anlegen und sicher verwahren
- ☐ Auslandstelefonie - nur für gewünschte Länder freigeben („teure Zonen aktivieren“)
- ☐ Kosten- oder Anruflimits beim Provider aktivieren
- ☐ Mitarbeitende zum Thema Social Hacking sensibilisieren und ggf. schulen lassen
- ☐ Regelmäßige Überprüfung der abgerechneten Verbindungen

Koordinierte Maßnahmen (erfordern Koordination mit der IT oder grundlegende Admin-Rechte)

- ☐ Voicemail-Zugänge mit sicheren PINs schützen
- ☐ Regelmäßige Firmware- und Softwareupdates durchführen (Telefone, Telefonanlage, SBC, Softphones etc.)
- ☐ Nicht benötigte Rufziele oder Länder sperren
- ☐ Anmeldung von Endgeräten auf bestimmte IP-Adresse oder TK-Anlage beschränken
- ☐ Zugriff auf Admin-Oberflächen nur aus dem internen Netz oder über VPN erlauben
- ☐ Firewalls so konfigurieren, dass nur erforderliche IPs und Ports freigegeben sind
- ☐ Portweiterleitungen (Port Forwarding) vermeiden, wo möglich
- ☐ Logs oder Dashboards der Telefonanlage regelmäßig prüfen
- ☐ Einsetzen von Virensoftware auf Clients
- ☐ Deaktivieren des SSH-Root-Zugriffs (falls verwendet; oft bei VM-Systemen relevant)
- ☐ Blockieren bzw. Deaktivieren von Diensten, die nicht benötigt werden

Strategisch-technische Maßnahmen (für IT-Fachpersonal oder externe IT-Dienstleister)

- ☐ SIP-Verbindungen per TLS verschlüsseln
- ☐ Sprachdaten per SRTP verschlüsseln
- ☐ Session Border Controller (SBC) zwischen Provider und Anlage einsetzen
- ☐ Nutzung offener SIP-Ports vermeiden oder nur in Verbindung mit IP-Restriktion
- ☐ Geoblocking, Rate-Limiting oder IDS-Funktionen aktiveren (sofern verfügbar)
- ☐ Anomaliererkennung oder Monitoring für Telefonieverkehrsdaten einrichten
- ☐ Endgeräte über VPN oder internes Netz registrieren – insofern möglich, nicht direkt über das Internet
- ☐ falls sicherheitsrelevanten Geräte in ein überwachtes Netzsegment einbinden

Weitere Informationen zum Thema IT-Sicherheit bzw. Cyber-Sicherheit finden Sie im jeweils Leitfaden zur Basis-Absicherung nach IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik.

VoIP-Sicherheitsleitfaden V2.1 (06/2025)

ansit-com GmbH
Lückstr. 72/73
10317 Berlin

Tel.: +49(0)30 208 477 960
Email: info@ansit-com.de

Web: https://www.ansit-com.de

LinkedIn: https://www.linkedin.com/company/ansit-com-gmbh/