ansitcom

VoIP-Telefonielösungen » individuell. flexibel. genial.

Sicherheitsleitfaden für VoIP Telefonie

ansitel

Sicherheitsleitfaden
Stand: Oktober 2020 (V2.1)

VoIP-Telefonielösungen » individuell. flexibel. genial.

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

Einleitung

Voice over IP hat sich in vielen Teilen der Erde zum Standard entwickelt und bringt für viele Unternehmen zahlreiche Vorteile mit. Wie nahezu alle rechner- oder internetgestützten Technologien, bringt jedoch auch die VoIP-Telefonie einige potenzielle Sicherheitsrisiken mit sich.

Es ist uns daher besonders wichtig, Sie über mögliche Risiken aufzuklären und Möglichkeiten aufzuzeigen, wie Sie sich vor diesen Gefahren schützen können. Bitte setzen Sie so gut wie möglich sämtliche Sicherheitsmaßnahmen um und kontaktieren Sie ggf. Ihren IT-Administrator oder IT-Dienstleister.

Gern stehen wir Ihnen für Fragen zu den Themen Datenschutz, Sicherheit und VoIP-Telefonie im Allgemeinen zur Verfügung.

V1.0 - 3_/3_/sec-guide-v1.afpub

Häufige Bedrohungen und Gefahren

Abhören bzw. Mithören von Gesprächen

Gespräche bei VoIP-Telefonaten werden über das Internet geführt. Durch Nutzung von Standardprotokollen, alten Firmwareständen in genutzten Endgeräten oder fehlerhaft konfigurierten Netzwerkinfrastrukturen können so genannte Sprachpakete abgefangen und schließlich zusammengesetzt werden. Dadurch ist ein Abhören von Gesprächen möglich.

Telefonanlagen-Hacking

Eine Telefonanlage ist das Herzstück der Telefonie. VoIP-Telefonanlagen können in der Regel über eine Weboberfläche konfiguriert und verwaltet werden. Enthält der Rechner, über den die Weboberfläche aufgerufen und sich eingeloggt wird Schadsoftware (Viren, Trojaner) können Hacker sich Zugriff zum Telefoniesystem verschaffen. Auch durch Verwendung unsicherer Passwörter steigt das Risiko eines unerwünschten Zugriffs. Durch das Hacking der Telefonanlage ist es möglich, kostenintensive Gespräche zu führen oder Endgeräte zu manipulieren.

DoS-Attacke

DoS steht für Denial of Service und bezeichnet eine Angriffsmethode auf ein Netzwerk, das mit großen Datenmengen geflutet wird. Wird eine solche Attacke mit einem Verbund aus mehreren Computern durchgeführt, bezeichnet man dies als DDos-Attacke (Distributed Denial of Service). Eine solche Attacke führt zur Überlastung eines Servers oder Netzwerks, was eine teilweise oder vollständige Nichterreichbarkeit zur Folge hat. Cloud-Telefonanlagen und Server von Telefonieprovidern sind von diesen Attacken am ehesten betroffen.

Diebstahl von SIP-Identitäten und Providerdaten

Durch den Diebstahl von SIP Zugangsdaten erhalten Hacker die Kontrolle über Ihren Telefonanschluss. Dadurch können Telefonate zu jedem beliebigen Ziel geführt werden. Ein solcher Diebstahl passiert meist durch Phishing über E-Mails, durch unsichere Passwortverwaltung oder durch den Diebstahl von Zugangsdaten. Werden SIP-Identitäten gestohlen, können unter Umständen hohe Kosten durch Telefongespräche ins Ausland entstehen.

Sicherheitsmaßnahmen

Sichere Passwörter und Passwortzugang

Verwenden Sie stets sichere Passwörter. Diese sollten möglichst aus Zahlen, großen und kleinen Buchstaben sowie Sonderzeichen bestehen. Achten Sie zudem auf die Passwortlänge. Je länger ein Passwort ist, umso schwieriger und zeitaufwändiger ist es, dieses zu hacken.

Bewahren Sie das Passwort an einem sicheren Ort auf und involvieren Sie so wenig wie möglich Personen. Empfehlenswert sind Passwortverwaltungstools wie z.B. Keypass. Speichern Sie Passwörter niemals im Browser.

Ändern der Passwörter

Es ist empfehlenswert Ihre Passwörter in bestimmten Zeitzyklen zu ändern. Nach Möglichkeit sollten Sie alle sechs Monate ein neues Passwort vergeben. Es ist auch angeraten, neue Passwörter zu vergeben, sowie neue Verantwortlichkeiten geregelt wurden (z.B. neuer Administrator, Weggang eines verantwortlichen Technikers).

Updates und Instandhaltung der Systeme

Telefonanlagen und Telefone werden im Rahmen ihrer Produktlaufheit permanent weiterentwickelt. Das schließt auch den Einbau neuer Sicherheitsfunktionen sowie Aktualisierung Von Sicherheitsdiensten (Security-Patches) mit ein. Stellen Sie daher sicher, dass sämtliche Geräte (Router, Firewalls, TK-Anlagen, Endgeräte, Betriebssysteme etc.) immer auf dem neuesten Stand sind.

Firewall

Eine Firewall ist ein Sicherungssystem, dass einen Rechner, ein Netzwerk oder ein anderes Gerät im Netzwerk (z.B. TK-Anlage) vor unerwünschten Zugriffen (vor allem über das Internet) schützt. Solche Firewalls können sowohl hardware- als auch softwarebasiert sein. Wir empfehlen grundsätzlich den Einsatz von Firewalls, um den Grad der Sicherheit zu erhöhen.

Tipp: Wenn Sie eine Firewall verwenden, geben Sie bitte nur die benötigten IP-Adressen und Ports Ihres Providers frei. Vermeiden Sie nach Möglichkeit die Nutzung von Portforwarding und sperren Sie ggf. nicht benötigte Subnetze.

Sicherheitsfunktionen bei Telefonieprovidern

Viele Provider ermöglichen eine Budgettierung bzw. die Angabe von Tages- oder Monatslimits. Insofern Sie Ihr tägliches Anrufvolumen einschätzen können, empfiehlt sich das Setzen eines festen Limits pro Tag. Sollte ein Angreifer einen Zugriff zu Ihrem Provider erhalten, ist der Schaden ausschließlich auf dieses Limit begrenzt. Einige Provider ermöglichen außerdem das Sperren von Ländern bzw. Ländervorwahlen.

Achten Sie bitte auf Ihre Passworthoheit und geben Sie weder den Benutzernamen noch Ihre Passwort in fremden Korrespondenzen an.

Innerhalb der ansitel Telefonanlage können Sie zudem in Ihrer Providereinstellung die Funktion „Teure Zonen deaktivieren“ klicken, insofern Sie keine Telefonie ins Ausland führen.

Verschlüsselung nutzen, wo möglich

Sowohl der Zugang zur Telefonanlage per Webbrowser, als auch der Telefonanschluss können unter Umständen verschlüsselt werden. Beispielsweise können sich VoIP-Telefone bei jeder beliebigen VoIP-Telefonanlage anmelden. Um dies zu vermeiden, kann man die Anmeldung auf eine bestimmte Telefonanlage beschränken (z.B. durch bestimmte Passwörter oder durch Setzen einer entsprechenden IP-Adresse im Endgerät).

Die meisten SIP-Provider nutzen TLS für die Signalverschlüsselung der Sprachpakete. Einige Provider ermöglichen die Verschlüsselung per SRTP, um Audio- und Videostreams zu kodieren. Dieser Verschlüsselungstyp ist ausschließlich für VoIP-Anrufe entwickelt worden.

Regelmäßige Backups

Bitte fertigen Sie regelmäßig Backups von Ihren Systemen sowie von der Konfiguration Ihrer Telefonanlage an. So haben Sie im Notfall immer eine funktionierende Version zur Verfügung und können Betriebsausfälle verhindern oder zumindest zeitlich minimieren. Bitte bewahren Sie diese Backups an einem separaten Ort auf

Checkliste

- [ ] Blockieren bzw. Deaktivieren von Diensten, die nicht benötigt werden
- [ ] Deaktivieren des SSH-Root-Zugriffs (falls verwendet)
- [ ] Installieren der VoIP-Anlagensoftware in einer sicheren Umgebung (z.B. bei Software-Appliances)
- [ ] Ändern der voreingestellten Passwörter in eigene und komplexe Kennwörter
- [ ] Regelmäßiges Ändern von Passwörtern
- [ ] Löschen von Zugängen ehemaliger Mitarbeiter(innen)
- [ ] Setzen einer PIN bei Konferenzen
- [ ] Beschränken des externen Zugriff auf bekannten IP-Adressen
- [ ] Beschränken von internationalen Anrufen bzw. Ländervorwahlen
- [ ] Sicherstellen, dass alle Netzwerkeinstellungen nur intern erreichbar sind
- [ ] Einsetzen einer Firewall
- [ ] Regelmäßiges Überprüfen / Monitoring des Firewall-Berichts
- [ ] Regelmäßige Überprüfung der abgerechneten Anrufe
- [ ] Einsetzen von Virensoftware auf Clients
- [ ] Setzen Sie, wo möglich, sichere Protokolle ein
- [ ] Regelmäßiges Überprüfen, ob Telefonanlage, Betriebssysteme, Browser und andere sicherheitsrelevante Anwendungen auf dem neuesten Stand sind

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.