AGFEO

Empfehlungen zum sicheren Betrieb von AGFEO Kommunikationslösungen

Sicherheit Ihrer AGFEO Telefonanlage – wichtige Hinweise und Empfehlungen
10. November2026LB – alle Angaben ohne Gewähr

So schützen Sie Ihr Kommunikationssystem vor unberechtigten Zugriffen und Telefonie-Missbrauch.

Moderne Telefonanlagen sind leistungsfähige IT-Systeme, die in bestehende Unternehmensnetzwerke eingebunden werden. Wie bei Computern, Servern und anderen vernetzten Geräten ist auch bei Kommunikationssystemen ein angemessenes Sicherheitskonzept erforderlich.

Insbesondere ungeschützte Zugriffe aus dem Internet, ungeeignete Netzwerkkonfigurationen, unsichere Zugangsdaten oder veraltete Softwarestände können Sicherheitsrisiken darstellen.

Eine mögliche Folge unberechtigter Zugriffe ist sogenannter Telefonie-Fraud: Dabei werden Telefonverbindungen ohne Zustimmung des Anschlussinhabers aufgebaut, beispielsweise zu kostenintensiven Auslands- oder Sonderrufnummern. Hierdurch können erhebliche Verbindungskosten entstehen.

Mit den folgenden Empfehlungen möchten wir Sie dabei unterstützen, Ihre AGFEO Kommunikationslösung sicher zu betreiben.

Wichtiges Prinzip:
Die Sicherheit eines Kommunikationssystems ergibt sich aus dem Zusammenspiel von aktueller Software, geeigneter Netzwerkkonfiguration, geschützten Zugängen und regelmäßiger Wartung.

1. Schützen Sie Ihre Telefonanlage vor direkten Zugriffen aus dem Internet!

Weder für die Kommunikation mit Ihrem Telefonie-Provider noch für die Nutzung unserer Apps von unterwegs oder die Fernwartung durch Ihren AGFEO Fachpartner müssen eingehende Ports in Ihrer Firewall freigegeben werden. Es sind keine eingehenden NAT-Portweiterleitungen notwendig!

Dennoch werden in der Praxis gelegentlich Portweiterleitungen in Routern oder Firewalls eingerichtet, beispielsweise für HTTP/HTTPS (Ports 80/443) oder SIP (Port 5060). Solche Freigaben können die Angriffsfläche eines Kommunikationssystems unnötig vergrößern.

Unsere ausdrücklichen Empfehlungen:

- Entfernen Sie sämtliche eingehenden NAT-Portweiterleitungen auf Ihre AGFEO Telefonanlage.
- Vermeiden Sie eine direkte öffentliche Erreichbarkeit der Administrationsoberfläche oder interner SIP-Dienste.
- Prüfen Sie hier insbesondere die Ports 5060, 80 und 443.

- Stellen Sie sicher, dass auch über IPv6 keine ungewollten Zugriffe aus dem Internet möglich sind.
- Nutzen Sie für die mobile App-Nutzung ausschließlich die vorgesehenen AGFEO RemoteApp-Dienste.
- Ermöglichen Sie Ihrem AGFEO Fachpartner den Fernzugriff über das AGFEO Fernwartungsportal.
- Lassen Sie Ihre Firewall-Konfiguration durch Ihren IT-Verantwortlichen oder AGFEO Fachpartner überprüfen.
- Nutzen Sie wann immer es geht, ausschließlich verschlüsselte Verbindungen.
- Bei Nutzung von lokalen on-premise TK-Systemen und Bedarf von Endgeräten an externen Standorten sind ausschließlich sichere VPN-Verbindungen anzuwenden.

Prinzip:
Eine aktuelle Firmware allein schützt nicht vor den Risiken unnötig öffentlich erreichbarer Dienste. Eine sichere Netzwerkkonfiguration ist deshalb unverzichtbar.

2. Firmware regelmäßig aktualisieren

Auch die Software Ihrer Telefonanlage benötigt regelmäßige Aktualisierungen. Neue Firmwareversionen enthalten neben funktionalen Weiterentwicklungen auch wichtige Sicherheitsverbesserungen und die Behebung bekannter Schwachstellen. AGFEO stellt für unterstützte Kommunikationssysteme regelmäßig Firmware-Aktualisierungen bereit. Diese können somit neben funktionalen Verbesserungen auch sicherheitsrelevante Anpassungen enthalten.

Unsere Empfehlung:

- Verwenden Sie stets einen aktuellen, für Ihr System freigegebenen Firmware- und Softwarestand.
- Beauftragen Sie Ihren AGFEO Fachpartner mit der regelmäßigen Überprüfung und Aktualisierung.
- Beachten Sie den Wartungsstatus Ihres Kommunikationssystems.

Für Produkte, deren reguläre Softwarepflege bereits eingestellt wurde (End of Maintenance – EoM), werden grundsätzlich keine regulären Firmware-Aktualisierungen mehr bereitgestellt. Bei entsprechenden Systemen empfehlen wir, gemeinsam mit Ihrem AGFEO Fachpartner eine Modernisierung zu prüfen.

- Für ausgewählte AGFEO Kommunikationssysteme stehen hierfür auch Upgrade-Kits zur Verfügung, mit denen vorhandene Installationen weitergenutzt und technisch aktualisiert werden können. https://agfeo.de/produkt/es-7xx-upgrade-kit/

- Alternativ bieten aktuelle AGFEO Kommunikationslösungen oder unsere HyperFonie Cloud-Telefonanlage entsprechende Modernisierungsmöglichkeiten.

3. Zusätzliche Schutzmaßnahmen gegen Telefonie-Fraud

Neben einem aktuellen Softwarestand und einer geschützten Netzwerkkonfiguration empfehlen wir weitere Sicherheitsmaßnahmen:

- Verwenden Sie individuelle, ausreichend starke Passwörter und ersetzen Sie unsichere oder voreingestellte Zugangsdaten.
- Ändern Sie Zugangsdaten unverzüglich, wenn der Verdacht besteht, dass diese unbefugten Personen bekannt geworden sind.
- Beschränken Sie Benutzerberechtigungen auf das jeweils erforderliche Maß.
- Lassen Sie nicht benötigte Funktionen und Zugänge deaktivieren.
- Vereinbaren Sie mit Ihrem Telefonie-Provider geeignete Kostenlimits, Benachrichtigungen und Sperren für kostenintensive Zielrufnummern.

- Nutzen Sie ergänzend die verfügbaren Sperr- und Berechtigungsmöglichkeiten Ihres AGFEO Kommunikationssystems.

Insbesondere providerseitige Kostenbegrenzungen können dazu beitragen, mögliche finanzielle Schäden durch missbräuchliche Telefonverbindungen zu begrenzen.

4. Was tun bei Verdacht auf einen unberechtigten Zugriff?

Wenn Sie ungewöhnliche Telefonverbindungen, unerklärliche Verbindungskosten oder Hinweise auf einen möglichen unberechtigten Zugriff feststellen, sollten Sie unverzüglich handeln.

Kontaktieren Sie Ihren Telefonie-Provider.
Lassen Sie verdächtige Verbindungen und gegebenenfalls betroffene Rufziele oder ausgehende Telefonieverbindungen sperren, um weitere Kosten zu vermeiden.

Informieren Sie Ihren betreuenden AGFEO Fachpartner.
Dieser kann gemeinsam mit Ihrer IT-Administration die Konfiguration, den Softwarestand und mögliche unberechtigte Zugriffe überprüfen.

Unterbinden Sie unsichere Zugriffswege.
Lassen Sie nicht erforderliche Portweiterleitungen deaktivieren und gegebenenfalls betroffene Systeme vom öffentlichen Internet isolieren. Berücksichtigen Sie dabei mögliche Auswirkungen auf die Erreichbarkeit Ihrer Telefonie.

Lassen Sie den Vorfall untersuchen.
Vor Veränderungen an der Konfiguration sollten vorhandene Protokolle und weitere relevante Informationen nach Möglichkeit gesichert werden. Dies kann für die technische Ursachenanalyse und die Klärung möglicher Schäden wichtig sein.

Stellen Sie einen sicheren Betriebszustand wieder her.
Hierzu gehören insbesondere die Überprüfung der Konfiguration, das Ersetzen möglicherweise kompromittierter Zugangsdaten, erforderliche Sicherheitsaktualisierungen und gegebenenfalls eine kontrollierte Neuinstallation oder Wiederherstellung. Erst nach entsprechender Prüfung sollte das betroffene System wieder uneingeschränkt betrieben werden.

5. Ihr AGFEO Fachpartner unterstützt Sie

Ihr betreuender AGFEO Fachpartner unterstützt Sie bei der Überprüfung und Absicherung Ihrer Installation sowie bei der Auswahl geeigneter Modernisierungsmöglichkeiten.

Einen qualifizierten AGFEO Fachpartner finden Sie unter www.agfeo.de/fachhaendlersuche.

6. Wichtiger Hinweis zur Betriebssicherheit und Haftung

Die Sicherheit einer Kommunikationslösung hängt neben den vom Hersteller bereitgestellten Sicherheitsfunktionen wesentlich von der ordnungsgemäßen Installation, Konfiguration, Wartung und Absicherung der jeweiligen IT- und Netzwerkumgebung ab.

Die Verantwortung für die sichere Konfiguration und den Betrieb der kundenseitigen Netzwerk- und Firewall-Infrastruktur liegt grundsätzlich beim jeweiligen Betreiber beziehungsweise den von ihm beauftragten IT-Dienstleistern.

AGFEO weist ausdrücklich darauf hin, dass für den vorgesehenen Betrieb seiner ES- und HyperVoice-Kommunikationssysteme keine eingehenden NAT-Portweiterleitungen aus dem öffentlichen Internet erforderlich sind. Insbesondere die Freigabe interner Dienste, beispielsweise über die Ports 5060, 80 oder 443, kann erhebliche Sicherheitsrisiken verursachen.

Für Schäden, die ausschließlich durch eine unsachgemäße Installation, eine unzureichend abgesicherte Betriebsumgebung, nicht erforderliche Portfreigaben oder sonstige vom Betreiber zu verantwortende Sicherheitsmängel entstehen und nicht auf eine von AGFEO zu vertretende Ursache zurückzuführen sind, übernimmt AGFEO keine Haftung.

Dies gilt insbesondere auch für finanzielle Schäden durch unberechtigte Telefonverbindungen (Telefonie-Fraud).

Zwingende gesetzliche Haftungsansprüche und eine etwaige Haftung von AGFEO für eigene Pflichtverletzungen bleiben hiervon unberührt.

==> Sichere Kommunikation beginnt mit einer sicheren Konfiguration!

Hinweis:
Alle Angaben Stand genanntem Datum, nur gültig zu den aufgelisteten Anlagensystemen und Firmwareversionen aber ohne Gewähr.