Sichere Telefonanlagen: Eigenschaften, Betrieb und organisatorische Maßnahmen

Die folgenden Hinweise unterstützen Unternehmen dabei, ihre Telefonanlage als Teil ihrer technischen und organisatorischen Sicherheitsmaßnahmen risikoorientiert zu bewerten. Sie können damit einen Beitrag leisten, Anforderungen aus NIS2 beziehungsweise der nationalen Umsetzung besser einzuordnen und umzusetzen. Eine abschließende rechtliche Bewertung oder Konformitätsprüfung ersetzen sie nicht.

Eine moderne Telefonanlage ist ein vernetztes IT-System. Sie verarbeitet Benutzerkonten, Berechtigungen, Ruf- und Verbindungsdaten, Konfigurationen, Schnittstellen sowie administrative Zugänge. Deshalb muss sie wie andere geschäftskritische IT-Systeme abgesichert, aktualisiert und dokumentiert werden.

Eine sichere Telefonanlage sollte insbesondere folgende Eigenschaften erfüllen:

Verschlüsselte Kommunikation
Administrative Zugänge, Verbindungen zu Endgeräten, Standortkopplungen, Cloud-Dienste, Fernwartung und Schnittstellen müssen verschlüsselt übertragen werden. Der Einsatz aktueller TLS-Versionen, geeigneter SRTP-Konfigurationen und sicherer kryptografischer Parameter ist dabei zentral. Der Einsatz aktueller TLS-Versionen und sicherer kryptografischer Parameter ist dabei zentral. Zertifikate und Kommunikationspartner müssen korrekt geprüft werden. Netzwerksegmentierung ersetzt Verschlüsselung nicht, sondern ergänzt sie.

Wirksame Zugriffskontrollen
Die Telefonanlage muss technisch durchsetzen, dass nur authentifizierte und autorisierte Personen bestimmte Funktionen ausführen können. Berechtigungen dürfen nicht nur über die Benutzeroberfläche gesteuert werden. Wichtig sind individuelle Benutzerkonten, Rollen- und Rechtekonzepte, getrennte Administrationsrechte und das Prinzip der geringstmöglichen Rechte.

Starke Authentifizierung
Passwortrichtlinien müssen technisch erzwungen werden. Standardpasswörter müssen bei Inbetriebnahme geändert oder verhindert werden. Für administrative Zugänge, Fernwartung, VPN- oder Cloud-Zugriffe ist Mehrfaktor-Authentifizierung als Mindestanforderung vorzusehen. Unterstützt die eingesetzte Lösung dies nicht, muss das Risiko dokumentiert und durch Ersatzmaßnahmen oder einen Wechsel adressiert werden.

Begrenzte Angriffsfläche
Es sollten ausschließlich für den Betrieb der Anlage erforderliche Dienste, Ports und Schnittstellen bereitgestellt werden. Nicht benötigte Dienste sind zu deaktivieren. Administrationsoberflächen sollten nicht unnötig aus dem Internet erreichbar sein. Externe Zugänge müssen durch Firewall-Regeln, VPN, Zugriffsbeschränkungen oder vergleichbare Maßnahmen abgesichert werden.

SIP- und Trunk-Sicherheit
Bei IP-Telefonie ist SIP besonders abzusichern. SIP-Ports werden häufig automatisiert gescannt; unzureichend geschützte SIP-Zugänge können Ziel von Brute-Force-Angriffen, manipulierten SIP-Nachrichten oder kostenintensivem Missbrauch von SIP-Trunks werden. Das ITK-System muss starke Authentifizierung für SIP-Zugänge erzwingen, fehlgeschlagene Registrierungen und auffällige Anrufversuche erkennen sowie Verbindungsversuche begrenzen. Verdächtige Muster sollten blockiert oder an ein Monitoring-System weitergeleitet werden. SIP- und RTP-Verkehr ist nach Möglichkeit verschlüsselt und nur aus definierten Netzen oder über gesicherte Provider-Anbindungen zuzulassen.

Sichere Speicherung von Daten
Konfigurationsdaten, Zugangsdaten, Backups, Zertifikate, Protokolle und sensible Kommunikationsdaten müssen gegen unbefugten Zugriff geschützt werden. Passwörter dürfen nicht im Klartext gespeichert werden. Backups müssen geschützt abgelegt und regelmäßig auf Wiederherstellbarkeit geprüft werden.

Update- und Wartungsfähigkeit
Regelmäßige Sicherheitsupdates sind verpflichtend und müssen einspielbar sein. Hersteller sollten Sicherheitshinweise, Härtungsempfehlungen, Angaben zum Produktlebenszyklus und klare Updateprozesse bereitstellen. Eine Anlage ohne verlässliche Sicherheitsupdates ist nicht sicher betreibbar.

Sichere Schnittstellen und Dateiimporte
Schnittstellen zu sollten nur über dokumentierte und abgesicherte Wege genutzt werden. Davon betroffen sind Drittsysteme, Konfigurationsimporte, Zertifikate, Ansagen, Backups oder Kontaktlisten. Nicht benötigte Integrationen sind zu deaktivieren. Dateiimporte sollten auf notwendige Formate begrenzt und nicht automatisch ausgeführt werden.

Was Unternehmen organisatorisch zusätzlich tun müssen

Sichere Produkteigenschaften reichen nicht aus. Unternehmen müssen den sicheren Betrieb organisatorisch absichern.

Verantwortlichkeiten festlegen
Es muss klar sein, wer für Administration, Benutzerkonten, Updates, Fernwartung, Dokumentation, Sicherheitsmeldungen und Abstimmung mit Systemhaus, Hersteller oder Provider verantwortlich ist.

Risiken dokumentieren
Die Telefonanlage muss Teil der IT-Risikobetrachtung sein. Auch ohne formales Informationssicherheitsmanagement sollten relevante Risiken schriftlich erfasst werden: externe Erreichbarkeit, Fernwartung, veraltete Softwarestände, fehlende Updates, unsichere Passwörter, offene Schnittstellen oder unklare Zuständigkeiten.

Benutzerkonten regelmäßig prüfen
Nicht mehr benötigte Konten sind zu löschen oder zu deaktivieren. Berechtigungen müssen regelmäßig geprüft und auf das notwendige Maß reduziert werden. Dies betrifft auch Gruppenfunktionen, Voicemail, mobile Apps, Softphones, Integrationskonten und externe Dienstleisterzugänge.

Fernwartung kontrollieren
Zur Kontrolle der Fernwartungszugänge zählt deren Dokumentation, ihre Absicherung und ihre ausschließlich bedarfsbedingte Aktivierung. Der Zugriff sollte nach Möglichkeit zeitlich begrenzt, mit Mehrfaktor-Authentifizierung geschützt und protokolliert sein. Nach Abschluss der Wartung ist der Zugang wieder zu deaktivieren.

Netzwerk absichern
Die Erreichbarkeit der Telefonanlage muss auf die nötigen Netzbereiche beschränkt sein. Administrationszugriffe sind auf berechtigte Personen, Geräte oder Netze zu begrenzen. Je nach Umgebung können VLANs, Firewall-Regeln, VPNs oder getrennte Administrationsnetze sinnvoll sein.

Updates verbindlich regeln
Es braucht einen festen Prozess für Sicherheitsupdates: Wer prüft Meldungen? Wer gibt Updates frei? Wer installiert sie? Wann wird getestet? Wie wird dokumentiert? Das gilt auch für Endgeräte, Softphones, Apps, Betriebssysteme und Zusatzkomponenten.

Offboarding sicherstellen
Beim Ausscheiden oder Rollenwechsel von Mitarbeitenden müssen Zugänge zur Telefonanlage angepasst oder deaktiviert werden. Dazu zählen Benutzerkonten, Administrationsrechte, Apps, Softphones, Voicemail, Weiterleitungen, Schlüssel und externe Zugänge.

Notfallfähigkeit vorbereiten
Unternehmen müssen festlegen, was bei Ausfall, Missbrauchsverdacht oder Cyberangriff zu tun ist. Erforderlich sind aktuelle Backups, Wiederherstellungsanleitungen, alternative Kommunikationswege und Notfallkontakte für Systemhaus, Hersteller und Provider.

Handlungsempfehlung: Betrieb, Updates, Verantwortlichkeiten, Dokumentation

Unternehmen können den sicheren Betrieb ihrer Telefonanlage in vier Schritten prüfen und absichern.

1. Bestand und Sicherheitsstatus erfassen
Zunächst muss dokumentiert werden, welche Telefonanlage eingesetzt wird, in welcher Version sie betrieben wird, wie sie angebunden ist, welche externen Zugänge bestehen und welche Systeme, Endgeräte, Apps und Schnittstellen verbunden sind. Ohne diese Bestandsaufnahme lässt sich das Sicherheitsniveau nicht belastbar bewerten.

2. Hersteller- und Systemhausinformationen einholen
Vom Hersteller oder betreuenden Systemhaus sollten Sicherheitshinweise, Härtungsempfehlungen, Updateinformationen, Angaben zum Produktlebenszyklus und empfohlene Netzwerkkonfigurationen eingeholt werden. Nach Umsetzung werden diese Informationen in der eigenen Dokumentation abgelegt.

3. Betrieb verbindlich regeln
Für Benutzerkonten, Berechtigungen, Fernwartung, Updates, Backups, Protokollierung und Notfallkontakte sollten klare Verantwortlichkeiten bestehen. Der Prozess muss auch dann funktionieren, wenn einzelne Personen nicht verfügbar sind.

4. Wechsel prüfen, wenn Sicherheitsanforderungen nicht erfüllt werden
Wenn eine Telefonanlage zentrale Sicherheitsanforderungen nicht erfüllt, keine verlässlichen Sicherheitsupdates mehr erhält oder nicht angemessen dokumentiert, gewartet und abgesichert werden kann, muss ein Wechsel auf eine moderne, sichere und updatefähige Lösung erfolgen.

Um die Cyber-Sicherheit zu wahren und regulatorische Anforderungen zu unterstützen, ist ein Wechsel auf eine moderne Lösung wie zum Beispiel die COMtrexx als On-Premise (lokal) oder die Cloud-Lösung COMuniq ONE des deutschen Herstellers Auerswald empfohlen. Ziel ist eine Migration mit möglichst geringem Aufwand, klarer Planung und nachvollziehbarer Verbesserung des Sicherheitsniveaus. Zwar stellt die Einführung eines Produktes auf dem Stand der Technik allein keine NIS2-Konformität her – sie bietet aber die technologische Voraussetzung. Letztlich entscheidend ist das Zusammenspiel aus sicherer Lösung, geeigneter Konfiguration, klaren Verantwortlichkeiten, dokumentiertem Betrieb und regelmäßigen Updates.

Checkliste: Telefonanlage auf Sicherheitsniveau prüfen

Prüffrage	Ja	Nein	Bemerkung
Liegt eine aktuelle Dokumentation der Telefonanlage vor?			
Sind Systemversion, Betriebsmodell, Schnittstellen und externe Zugänge dokumentiert?			
Werden administrative und relevante technische Verbindungen verschlüsselt übertragen?			
Werden aktuelle TLS-Versionen und sichere kryptografische Verfahren genutzt?			
Sind unsichere oder veraltete Protokolle deaktiviert?			
Sind nur notwendige Dienste, Ports und Schnittstellen erreichbar?			
Sind SIP-Zugänge gegen automatisiertes Scanning, Brute-Force-Angriffe und missbräuchliche Nutzung geschützt?			
Ist die Administrationsoberfläche ausreichend vor externem Zugriff geschützt?			

Prüffrage	Ja	Nein	Bemerkung
Gibt es individuelle Benutzer- und Administrationskonten?			
Werden starke Passwörter technisch erzwungen?			
Wird Mehrfaktor-Authentifizierung für kritische Zugänge genutzt, sofern verfügbar?			
Werden Benutzerkonten und Berechtigungen regelmäßig geprüft?			
Sind nicht mehr benötigte Konten deaktiviert oder gelöscht?			
Sind Fernwartungs- und Supportzugänge dokumentiert?			
Werden Fernwartungszugänge nur bei Bedarf aktiviert?			
Werden sicherheitsrelevante Ereignisse protokolliert?			
Werden fehlgeschlagene SIP-Registrierungen und auffällige Anrufversuche erkannt, begrenzt oder an ein Monitoring weitergeleitet?			
Werden Sicherheitsupdates zeitnah eingespielt?			
Gibt es einen dokumentierten Update- und Wartungsprozess?			
Sind Härtungs- und Sicherheitsempfehlungen des Herstellers umgesetzt?			
Werden Backups geschützt gespeichert und regelmäßig getestet?			
Sind mobile Endgeräte, Softphones und Apps in das Sicherheitskonzept einbezogen?			
Gibt es ein geregeltes Offboarding für Telefonanlagenzugänge?			
Sind Notfallkontakte auch bei IT-Ausfall verfügbar?			
Ist geklärt, wie bei Sicherheitsvorfällen vorzugehen ist?			
Ist bekannt, bis wann die Anlage Sicherheitsupdates erhält?			
Wurde bewertet, ob die Anlage weiterhin sicher betrieben werden kann?			