



Checkliste:

Sicherheitsstatus einer Telekommunikationsanlage

Mit dem Betrieb von Telekommunikationsanlagen (TK-Anlagen) steht dem Anwender ein leistungsfähiges Kommunikationssystem für die Übertragung und Speicherung von Sprache, Text, Bild und Daten zur Verfügung. Bei der Multifunktionalität einer solchen Anlage kann jedoch ein Ausfall die gesamte innerbetriebliche Kommunikation lahm legen. Deshalb muss der Sicherheit des Kommunikationssystems der gleiche Stellenwert wie der sonstiger DV-Anlagen eingeräumt werden.

Bei der nachfolgenden Analyse wird ganz besonderer Wert auf die Erstellung einer übersichtlichen Installationsdokumentation gelegt. Häufig ist es so, dass die für den Betrieb der TK-Anlage zuständigen Personen keinen Überblick über den Umfang der Leistungsmerkmale und die Schutzmechanismen der Kommunikationsanlage haben. Eine Risiko- und Bedrohungsanalyse ist dann nicht mehr machbar. Auch kommt es vor, dass der Hersteller mit der Einrichtung, Verwaltung und Wartung der Kommunikationsanlage betraut und in der Behörde dafür wohl aus falsch verstandener Sparsamkeit kein Know-how aufgebaut wurde. Auch die Aspekte des Datenschutzes werden beim Betrieb von TK-Anlagen häufig vernachlässigt.

Analyse des Sicherheitsstatus einer TK-Anlage

Eine TK-Anlage unterstützt eine Vielzahl von Kommunikationsdiensten, so dass man sich vor der Installation und der Generierung genau überlegen muss, welche Teilnehmer welche Berechtigungen erhalten sollen und wie ein ordnungsgemäßer Betrieb der Kommunikationsanlage sicherzustellen ist. Die nachfolgende Checkliste soll dabei helfen. Vor allem aber soll sie als Hilfsmittel zur Dokumentation und als Prüfungsunterlage für die Revision dienen. Bei den Sicherheitsmaßnahmen wird zwischen Ist- und Sollmaßnahmen unterschieden. Auf diese Weise eignet sich diese Darstellung auch für Fortschreibung.



1. Beschreibung der Installation

1.1 Allgemeines

Behörde:

Hersteller der Anlage:

Bezeichnung der Anlage:

1.2 Zeitpunkt der Installation

Wann wurde die TK-Anlage für den Echtbetrieb freigegeben?

Datum:

1.3 Endgeräte

Aufzählung der Endgeräte nach Typ und Anzahl. Die Zeilen sind bei Bedarf zu wiederholen.

Typ: Anzahl:

Typ: Anzahl:

1.4. Leistungsmerkmale

Nachfolgend werden einige Leistungsmerkmale aufgezählt, die für TK-Anlagen möglich sind. Es sind hier diejenigen auszuwählen, die für mindestens ein Endgerät aktiviert wurden. Alle restlichen nicht benützten Leistungsmerkmale sind zu streichen.

Anmerkung: Gegebenenfalls ist diese Liste auch um zusätzliche, hier fehlende Merkmale zu ergänzen.

1.4.1 Leistungsmerkmale für den Teilnehmer

- Automatischer Rückruf
 - im Besetztfall
 - im Freifall
- Rückrufsschutz
- Rückfrage
- Makeln (Rufweiterschaltung nach Rücksprache mit dem Teilnehmer)
- Briefkasten
- Wahlwiederholung (Speicherung der zuletzt gewählten Rufnummer)
- Zentrale und individuelle Kurzwahl
- Anrufumleitung
 - auf eine interne oder externe Sprechstelle
 - auf einen Teletex-Empfangspeicher



- auf ein Fax-Gerät
- auf einen Datenkommunikationsanschluss
- in eine Info-Box
- Anrufübernahme innerhalb einer Gruppe oder gezielt
- Dreier- oder Mehrfachkonferenz
- Direktruf
- Halten bzw. Parken einer Verbindung, bis die gewünschte Sprechstelle frei ist
- Zugriff auf eine Info-Box
 - für Sprachnachrichten
 - für Textnachrichten
 - für Fax-Nachrichten
- Direktansprechen und –antworten über den integrierten Lautsprecher bzw. das Mikrofon
- Ansprechschutz, um ungewolltes Mithören zu vermeiden
- Termineinrichtung (automatischer Anruf zu festgelegten Zeiten)
- Anrufschutz
- Anklopfen bei einem besetzten Teilnehmer
- Aufschalten auf einen besetzten Teilnehmer
- Anklopf- und Aufschaltschutz
- Anschluss von privaten Sondereinrichtungen (Lautsprecher, Ansagegeräte, Personensucheinrichtungen)
-
-

1.4.2 Sonstige Leistungsmerkmale

- Integrierte Vorzimmeranlage
- Rufweeterschaltung
 - an Teilnehmeranschluss
 - an Vermittlung oder Sammelanschluss
 - in einen Sprachspeicher
 - an eine Fax-Infobox
- Individuelle Kurzwahl
- Elektronisches Telefonbuch
- Mobile Teilnehmeridentifizierung durch Chipkarte (SmartCard) oder PIN-Eingabe
- Definition von Sammelanschlüssen
 - mit Gruppenbildung
- Amts- oder Fernamtsberechtigungen
 - Einrichtung von Berechtigungsklassen



- Berechtigungsumschaltung
- Selbsttätiger Verbindungsaufbau
- Vermitteln von Amtsverbindungen
- Displayanzeige
 - permanent
 - ab- oder zuschaltbar (unterdrückbar)
-
-

1.4.3 Systemfunktionen

- Gebührenerfassung
- Freizügige Nummerierung (Teilnehmerkennzeichnung durch Chipkarte und PIN)
- Wahlkontrolle für externe Verbindungen
- Fangen eines Anrufes (Protokollierung der Rufnummer eines Anrufers)
- Netz- und Batteriebetrieb
- Wiederholung von Alarmsignalen (die Alarmsignalisierung in der Zentrale kann an anderen Stellen wiederholt werden.)
- Amtsumschaltung bei Spannungsausfall
- Serverdienste (FAX, X.400, Bildschirmtext, Internet- oder sonstiger Datennetzanschluss)
- Mehrwert- und Informationsdienste
- Fernwirkdienste (z.B. Wartung)
-
-

1.4.4 Dokumentation

Existiert eine Dokumentation, welche Nebenstelle über welche Leistungsmerkmale verfügt?

nein/ja (als Anlage beigefügt)

.....

1.5 Zuständigkeiten

Auflistung der Personen, die für den Betrieb der Nebenstellenanlage verantwortlich sind. (Diese Informationen sind entsprechend der Personenzahl zu wiederholen).

Name: seit:

Rufnummer:

Name: seit:



Rufnummer:

1.6 Anschluss an IT-Systeme

Bezeichnung der DV-Anlagen, die an die TK-Anlage angeschlossen sind. Gegebenenfalls sind zusätzliche Einträge zu machen.

- Arbeitsplatzcomputer
Modell: Standort:
Zusätzliche Angaben:
- Gebührencomputer
Modell: Standort:
Zusätzliche Angaben:
- Netzwerkserver
Modell: Standort:
Zusätzliche Angaben:
- Hostrechner
Modell: Standort:
Zusätzliche Angaben:

Existiert ein entsprechender Konfigurationsplan?

nein/ja (als Anlage beigelegt)

.....

2. Aspekte der Datenspeicherung

2.1 Dateiarnten

Bezeichnung der (personenbezogenen) Informationen, die in Verbindung mit der TK-Anlage gespeichert werden.

- Leistungsmerkmale je Nebenstelle
- Kurzwahlregister
 - . allgemein
 - . individuell
- Elektronisches Telefonbuch
- Protokolldaten (Verbindungsdaten)
- Abrechnungsdaten
- Sprachspeicher



-
-

2.2 Dienstvereinbarung

Bezeichnung des Verfahrens, für welches eine Dienstvereinbarung bezüglich der TK-Anlage abgeschlossen wurde.

Verfahren:

Datum:

Bemerkungen:

2.3 Verfahrensfreigaben

Aufzählung der im Zusammenhang mit der TK-Anlage datenschutzrechtlich freigegebenen Verfahren. Jedes Verfahren ist gesondert zu erfassen.

Verfahren:

Datum:

Bemerkungen:

Verfahren:

Datum:

Bemerkungen:

2.4 Löschungen von gespeicherten Daten

Dokumentation der Lösungsfristen für jede Art einer Datenspeicherung (jedoch nur datei-bezogen). Gibt es geeignete Löschroutinen?

Datei:

Speicherungsdauer:

Bemerkungen:

Durchführung der Löschung:

Datei:

Speicherungsdauer:

Bemerkungen:

Durchführung der Löschung:



2.5 Nutzung von Personendaten

Angabe der Stellen und der Aufgaben, für die die Daten verarbeitet werden. Jede Datei ist gesondert zu behandeln.

Datei:

Stelle/Abteilung:

Zweck:

Datei:

Stelle/Abteilung:

Zweck:

2.6 Zweckbindung

Durch welche Maßnahmen wird die Zweckbindung solcher Datennutzungen sichergestellt?

Istmaßnahmen:

seit:

Bewertung:

Sollmaßnahmen:

Termin:

Bewertung:

2.7 Weiterleitung von Gebührendaten

An welche Stellen werden Gebührendaten in welcher Form weitergeleitet? Jede Weitergabe ist gesondert zu beschreiben.

Empfänger:

Daten(träger)art:

Zweck:

Datenumfang:

Löschungsbemerkung:

Empfänger:

Daten(träger)art:

Zweck:

Datenumfang:



Löschungsbemerkung:

2.8 Sonstige Datenschutzmaßnahmen

Bedarf an Datenschutzmaßnahmen gegenüber Dritten:

- *Anonymität des Anrufenden bei „besonderen“ Beratungsstellen (Endgeräte ohne Display oder Unterdrückung der Rufnummernanzeige)*
- *Akustisches Signal beim Aufschalten auf bestehende Verbindungen*
- *Schutz des Angerufenen bei Anrufumleitung*
- *Mithören Dritter über Mithöreinrichtungen oder Konferenzschaltung nur nach Zustimmung des Gesprächspartners (Problem der Zeugenzuschaltung)*
- *Anzeige beim Aufzeichnen von Gesprächsinhalten*
-
-

2.9 Benutzerordnung

Durch welche Richtlinien ist die Benutzung der TK-Anlagen durch die Mitarbeiter geregelt?

Richtlinie:

vom:

3. Sicherheitsmaßnahmen

3.1 Sicherheitsrichtlinie

Gibt es eine Sicherheitsrichtlinie, die insbesondere folgende Bereiche regelt:

- Installation, Betrieb und Wartung der TK-Anlage sowie der Endgeräte
- Dokumentation der Funktionalität (Transparenz)
- Inanspruchnahme von externen Dritten
- Schutzmaßnahmen für gespeicherte Daten
- Abschottung der Zugänge zu offenen Systemen (z.B. X.400, Internet)
- Schulung aller Benutzer

3.2. Betriebsterminal, Zentraleinheit und Knotenpunkte

3.2.1 Aufstellungsort

Wo sind das Betriebsterminal, die Zentraleinheit und eventuell vorhandene Knotenpunkte installiert?

Ort:



3.2.2 Schutzmaßnahmen

Durch welche Schutzmaßnahmen (z. B. Alarmüberwachung) sind Betriebsterminal und Zentraleinheit gegen den Zugriff Unberechtigter gesichert?

Istmaßnahmen:

seit:

Bewertung:

Sollmaßnahmen:

Termin:

Bewertung:

3.2.3 Zugangsberechtigte

Wer hat Zugang zum Betriebsterminal, zur Zentraleinheit und zu eventuell vorhandenen Knotenpunkten und wann wurden ihm die Zugangsrechte verliehen? Jede Person ist gesondert aufzuführen.

Name:

seit:

Rufnummer:.....

Name:

seit:

Rufnummer:.....

Name:

seit:

Rufnummer:.....

3.2.4 Erteilung der Zugangsberechtigung

Welche Personen sind seit wann für die Erteilung der Zugangsberechtigung zuständig?

Name:

seit:

Rufnummer:.....

Name:

seit:



Rufnummer:.....

Name:

seit:

Rufnummer:.....

3.2.5 Sicherung der Datenträger mit Gebührendaten

Durch welche Maßnahmen wird der unberechtigte Zugriff auf Datenträger mit Gebührendaten unterbunden?

Istmaßnahmen:

seit:

Bewertung:

Sollmaßnahmen:

Termin:

Bewertung:

3.2.6 Brandschutzmaßnahmen

Welche Brandschutzmaßnahmen (z. B. Schaffung eines eigenen Brandabschnittes, Alarmüberwachung, Feuerlöscher) wurden ergriffen?

Istmaßnahmen:

seit:

Bewertung:

Sollmaßnahmen:

Termin:

Bewertung:

3.3. Administrierung der Anlage

3.3.1 Zugangsberechtigte

Welche Personen verfügen seit welchem Zeitpunkt über eine Systemzugangsberechtigung?

Name:

seit:

Rufnummer:.....



Name:

seit:

Rufnummer:.....

Name:

seit:

Rufnummer:.....

3.3.2 Erteilung der Zugangsberechtigung

Wer ist für die Erteilung der Zugangsberechtigung zum System zuständig?

Name:

seit:

Rufnummer:.....

Name:

seit:

Rufnummer:.....

Name:

seit:

Rufnummer:.....

3.3.3 Zugriffsschutzmaßnahmen

Durch welche Maßnahmen wird der Zugriffsschutz realisiert?

Mögliche Maßnahmen wären beispielsweise:

- *Änderung der Installations- und Transportpassworte*
- *Einrichtung von Passworten*
- *Einrichtung von Doppelpassworten (nach dem Vier-Augen-Prinzip)*
- *Verwendung von Chipkarten (SmartCards)*
- *Verwendung einer PIN*
- *Einsatz biometrischer Verfahren*
- *verschlüsselte Abspeicherung der Anwenderdaten*

Istmaßnahmen:

seit:



Bewertung:

Sollmaßnahmen:

Termin:

Bewertung:

3.3.4 Systemverwaltung

Welche Aufgaben nimmt die Systemverwaltung wahr (Auswertung von Protokolldaten, Einrichten von Benutzern, Zuordnung von Leistungsmerkmalen, Behebung von Fehlern etc.)?

Aufgaben:

-
-
-
-
-

3.3.5 Schulungsmaßnahmen

Sind die betreffenden Benutzer hinsichtlich der gebotenen Sicherheitsmaßnahmen ausreichend geschult (Passwortänderung, Protokollüberprüfung, Verhinderung von Gebührenbetrug etc.)?

ja /nein

Bedarf besteht für:

3.4. Wartung und Fernwartung

3.4.1 Vertragliche Regelungen

Seit wann bestehen Vereinbarungen über die Wartung, wer sind der Auftraggeber und die Auftragnehmer (eventuell sogar Verzicht auf Fernwartung)?

Auftraggeber:

Auftragnehmer:

Vertrag vom:

3.4.2 Wartungsberechtigte

Wer ist für die Wartung bzw. Fernwartung zuständig?



Wartung vor Ort:

Namen:

.....

Rufnummern:

Fernwartung:

Namen:

.....

Rufnummern:

Sitz der Wartungszentrale:

3.4.3 Zugriffsschutzmaßnahmen

Welche Zugriffsschutzmaßnahmen sind für die Wartung vorgesehen?

Mögliche Maßnahmen wären beispielsweise:

- *Wartung wird nur nach Freigabe durch den Betreiber aktiv*
- *Passwortschutzverfahren (Doppelpasswort, SmartCard)*
- *eingeschränkter Zugriff (nur auf Systemdaten)*
- *Verbindungsaufbau durch Rückruf*
- *Wartung unter Aufsicht*

Istmaßnahmen:

seit:

Bewertung:

Sollmaßnahmen:

Termin:

Bewertung:

3.5 Schutz der Leitungswege

Durch welche Maßnahmen wird ein Manipulieren der Leitungswege verhindert?

Mögliche Maßnahmen wären z.B.:

- *plombierte Kabelschächte*
- *gesicherte Verteiler (Knoten)*
- *Verschlüsselung der Nachrichten*
- *alarmüberwachte Leitungsschächte*

Istmaßnahmen:



seit:

Bewertung:

Sollmaßnahmen:

Termin:

Bewertung:

3.6 Organisation der Telekommunikationsdienste

3.6.1 Elektronischer Versand von Dokumenten

Beim elektronischen Versand von Dokumenten ist insbesondere auf die Einhaltung folgender Maßnahmen zu achten:

- Maßnahmen gegen unbefugte Einsichtnahme
- Prüfung der Korrektheit der Zustellung an den Adressaten
- Selbstschutz gegen elektronisch übertragenes Werbematerial
-
-

3.6.2 Mehrwert- und Informationsdienste

Bei Öffnung der TK-Anlage für Mehrwert- und Informationsdienste ist darauf zu achten, dass ihr Zugang nur den dafür privilegierten Personen möglich ist.

Welcher Personenkreis hat welche Rechte?

Dienst:

Personenkreis:

Dienst:

Personenkreis:

Dienst:

Personenkreis:

3.7 Revision der Aktivitäten

Durch welche Dokumentationen bzw. Aufzeichnungen ist die ordnungsgemäße Verwendung der Kommunikationsanlage zu überprüfen?

Mögliche Maßnahmen wären u.a.:

- *Protokollierung jedes Systemzugangs*
- *Zwangsprotokollierung aller Administratoraktivitäten*



- *vollständige Zwangsprotokollierung der Fernwartungsaktivitäten*
- *Dokumentation aller zugelassenen Leistungsmerkmale je Endgerät*
- *Löschungsschutz der Protokolldaten*
- *Protokollierung der Datenzugriffe in Abhängigkeit von der Zugriffsart*

Istmaßnahmen:

seit:

Bewertung:

Sollmaßnahmen:

Termin:

Bewertung:

3.8 Schutz der Endgeräte

Durch welche Maßnahmen werden die Endgeräte gegen unberechtigte Inbetriebnahme geschützt?

Mögliche Maßnahmen wären beispielsweise:

- *Abschließen der Räume*
- *mechanisches Schloss, Unterbrechung der Stromzufuhr*
- *Sperrung durch Hardwareschloss*
- *Sperrung durch Softwareschloss (Codeeingabe vor Inbetriebnahme)*
- *Chipkarten-Einsatz*

(Die Maßnahmen sollten sich an der Funktionalität der Endgeräte orientieren.)

Istmaßnahmen:

seit:

Bewertung:

Sollmaßnahmen:

Termin:

Bewertung:

3.9. Notfallkonzept

3.9.1 Notfallhandbuch

Existiert ein aktuelles Notfallhandbuch, in dem alle im Notfall notwendig werdenden Aktionen enthalten sind?



ja/nein

Stand:.....

Zuständigkeit:

Name:

Rufnummer:

3.9.2 Aktionsplan

Wer ist im Notfall zu verständigen?

Name:

Adresse:

Rufnummer:.....

Name:

Adresse:

Rufnummer:.....

Name:

Adresse:

Rufnummer:.....

3.9.3 Backup-Ressourcen

Sind mehrere TK-Anlagen im Einsatz, so dass bei Ausfall einer TK-Anlage auf eine andere umgeschaltet werden kann?

ja/nein

*Sind mit dem Hersteller oder anderen Firmen schriftliche Vereinbarungen über die Ersatzge-
stellung von benötigten Backup-Ressourcen getroffen worden?*

ja/nein

Vertrag vom:

mit:

Maßnahmen:

3.9.4 Maßnahmen zur Sicherstellung der Verfügbarkeit

Existieren besondere Maßnahmen zur Sicherstellung der Verfügbarkeit?



Mögliche Maßnahmen wären beispielsweise:

- *USV-Anlage*
- *Überspannungsschutz*

Istmaßnahmen:

seit:

Bewertung:

Sollmaßnahmen:

Termin:

Bewertung:

4. Kontrolle der Sicherheitsmaßnahmen und der Dokumentation

Wer ist für die Kontrolle der Einhaltung der Sicherheitsmaßnahmen und der Dokumentation zuständig und welches Ergebnis brachten diese Kontrollen?

Name:

Datum:

Ergebnis:

.....

Nächste Kontrolle:

Anmerkungen:

Bei den vorgeschlagenen Maßnahmen handelt es sich um eine beispielhafte Aufzählung, die keinen Anspruch auf Vollständigkeit erhebt. Bei manchen Fragestellungen können auch mehrere Maßnahmen zweckmäßig sein.