|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Sicherheitsrichtlinie "TK-Anlage"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300042 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "TK-Anlage" | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc81724579)

[Dokumentenhistorie 3](#_Toc81724580)

[Inhaltsverzeichnis 4](#_Toc81724581)

[Allgemeine Festlegungen 5](#_Toc81724582)

[Ziel / Zweck 5](#_Toc81724583)

[Geltungsbereich 5](#_Toc81724584)

[Zuständigkeiten 5](#_Toc81724585)

[Genehmigungs- und Änderungsverfahren 6](#_Toc81724586)

[Aufbau des Dokuments 6](#_Toc81724587)

[Sicherheitsrichtlinie „TK-Anlage" 7](#_Toc81724588)

[Basismaßnahmen 7](#_Toc81724589)

[Anforderungsanalyse und Planung für TK-Anlagen (NET.4.1.A1) 7](#_Toc81724590)

[Auswahl von TK-Diensteanbietern (NET.4.1.A2) 7](#_Toc81724591)

[Änderung voreingestellter Passwörter (NET.4.1.A3) 8](#_Toc81724592)

[Absicherung von Remote-Zugängen (NET.4.1.A4) 8](#_Toc81724593)

[Protokollierung bei TK-Anlagen (NET.4.1.A5) 8](#_Toc81724594)

[Standardmaßnahmen 8](#_Toc81724595)

[Aufstellung der TK-Anlage (NET.4.1.A7) 8](#_Toc81724596)

[Einschränkung und Sperrung nicht benötigter oder sicherheitskritischer Leistungsmerkmale (NET.4.1.A8) 9](#_Toc81724597)

[Schulung zur sicheren Nutzung von TK-Anlagen (NET.4.1.A9) 9](#_Toc81724598)

[Dokumentation und Revision der TK-Anlagenkonfiguration (NET.4.1.A10) 10](#_Toc81724599)

[Außerbetriebnahme von TK-Anlagen und –Geräten (NET.4.1.A11) 10](#_Toc81724600)

[Datensicherung der Konfigurationsdateien (NET.4.1.A12) 10](#_Toc81724601)

[Beschaffung von TK-Anlagen (NET.4.1.A13) 10](#_Toc81724602)

[Notfallfürsorge für TK-Anlagen (NET.4.1.A14) 10](#_Toc81724603)

[Notrufe bei einem Ausfall der TK-Anlage (NET.4.1.A15) 11](#_Toc81724604)

[Sicherung von Telefonie-Endgeräten in frei zugänglichen Räumen (NET.4.1.A16) 11](#_Toc81724605)

[Wartung von TK-Anlagen (NET.4.1.A17) 11](#_Toc81724606)

[Maßnahmen bei erhöhtem Schutzbedarf 11](#_Toc81724607)

[Erhöhter Zugriffsschutz (NET.4.1.A18 - CA) 12](#_Toc81724608)

[Redundanter Anschluss (NET.4.1.A19 - A) 12](#_Toc81724609)

# Allgemeine Festlegungen

## Ziel / Zweck

Mit einer Telekommunikationsanlage, kurz TK-Anlage, können die Telefone der <Institution> intern verbunden und extern an ein öffentliches Telefonnetz angeschlossen werden. Durch die zunehmende Verzahnung von IT und Telekommunikation können TK-Anlagen dabei sowohl analog als auch IP-basiert aufgebaut sein. Hybrid-Anlagen sind eine Kombination aus einer klassischen Telekommunikationslösung und einem VoIP-System. Mit einer Hybrid-Anlage können klassische digitale und analoge Telefonie sowie VoIP gleichzeitig betrieben werden.

Neben der Sprachtelefonie können, abhängig von den angeschlossenen Endgeräten, weitere Dienste genutzt werden. So ist es möglich, mittels TK-Anlagen Daten, Texte, Grafiken und eine Folge von Bildern (bewegte Bilder) zu übertragen. Die Informationen können dabei analog oder digital über drahtgebundene oder drahtlose Übertragungsmedien weitergeleitet werden.

Das Ziel der Sicherheitsrichtlinie ist der Schutz der Informationen, die über TK-Anlagen übermittelt werden sowie der Schutz der Anlage vor Fremdeingriffen und Manipulationen. Bei der Erstellung dieser Sicherheitsrichtlinie wurden die Vorgaben des BSI Bausteines NET.4.1 "TK-Anlagen" beachtet.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Die Sicherheitsrichtlinie „TK-Anlage“ wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie „TK-Anlage"

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

### Anforderungsanalyse und Planung für TK-Anlagen (NET.4.1.A1)

Vor der Beschaffung oder Erweiterung einer TK-Anlage ist eine Anforderungsanalyse durchzuführen. Bei neu zu beschaffenden TK-Anlagen sind im Rahmen der Analyse die erwünschten Funktionen der TK-Anlagen festzulegen. Hierbei sind folgende Aspekte zu beachten:

* In welcher Ausprägung soll die TK-Infrastruktur genutzt werden:
  + Als klassische TK-Anlage,
  + Als VoIP-System oder
  + Als Hybrid-Anlage?
* Wie viele Anschlüsse soll die TK-Infrastruktur verwalten können?
* Lässt sich diese Anzahl nach dem Kauf noch erhöhen?
* Wie wird die Anbindung ans öffentliche Telefonnetz (PSTN/TDM oder SIP) erfolgen?
* Wie viele Gespräche sollen gleichzeitig geführt werden oder soll diese variabel nach Bedarf gestaltet werden können?
* Wie viele interne Kommunikationsverbindungen sollen gleichzeitig möglich sein?
* Wie viele externe Kommunikationsverbindungen ins öffentliche Netz sollen gleichzeitig möglich sein?
* Welche Aufgaben soll die zu neue TK-Infrastruktur erfüllen?
  + Welche Funktionen sollen bereitgestellt werden?
  + Welche Funktionen sind zwingend bereitzustellen?
  + Können vorhandene Endgeräte alle geforderten Funktionen im Zusammenspiel mit der TK-Infrastruktur und den Anforderungen der Arbeitsplatz zur Verfügung stellen?
  + Genügt eine eventuell bereits vorhandene Verkabelung den Anforderungen der TK-Anlage oder muss die Verkabelung erneuert werden?
  + Gibt es besondere Anforderungen an die Verfügbarkeit der TK-Infrastruktur oder an die Vertraulichkeit oder Integrität der gespeicherten oder verarbeiteten Gesprächsdaten?
* Wie wird die Sicherheit der TK-Infrastruktur (Zutritt und Zugriff), des Telefonnetzes und der Endgeräte gewährleistet?
* Ist ein Service- oder Wartungsvertrag für die TK-Infrastruktur notwendig oder können die benötigten Skills durch die <Institution> selbst bereitgestellt werden?
* Welche maximal tolerierbare Ausfallzeit und welche Wiederherstellungszeit werden benötigt unter Berücksichtigung der vereinbarten SLA- und OLA-Werte?

### Auswahl von TK-Diensteanbietern (NET.4.1.A2)

Um mit Personen telefonieren zu können, die nicht an der TK-Infrastruktur der <Institution> angeschlossen sind, ist mittels eines Vertrags ein öffentlicher Anbieter für Telefonie (PSTN- bzw. SIP-Provider) zu beauftragen. Dabei sind die Anforderungen der internen Sicherheitsrichtlinien sowie vertragliche und finanzielle Aspekte zu berücksichtigen. Alle vereinbarten Leistungen sind genau und eindeutig zu dokumentieren.

### Änderung voreingestellter Passwörter (NET.4.1.A3)

Vor Inbetriebnahme der Komponenten der TK-Infrastruktur sind alle Standardpasswörter durch ausreichend starke Passwörter zu ersetzen und vordefinierte Logins sofern möglich zu ändern oder zu löschen.

Bei den eingesetzten TK-Komponenten vorgenommene Änderungen der Konfiguration sind im Anschluss Datensicherungen durchzuführen.

### Absicherung von Remote-Zugängen (NET.4.1.A4)

Es ist zu prüfen, ob interne oder externe Remote-Zugänge zur TK-Anlage benötigt werden. Die externe Fernwartung bei klassischen TK-Anlagen sollte dabei nach Möglichkeit unterbunden werden. Alle nicht benötigten Remote-Zugänge sind zu deaktivieren. Alle anderen Remote-Zugänge sind vor unberechtigtem Zugriff zu schützen und auf die notwendigen Personen (Need-to-know Prinzip) zu beschränken.

### Protokollierung bei TK-Anlagen (NET.4.1.A5)

Die betriebene TK-Infrastruktur muss eine zielgruppenorientierte Protokollierung sicherstellen. Die Protokollierung der Servicenutzung sollte mindestens die Informationen enthalten:

* Zeit und Datum eines Gespräches oder einer Verbindung,
* Quell- und Zielrufnummer bzw. Quell- und Ziel-IP-Adresse sowie die
* Gesprächsdauer.

Im Rahmen der Protokollierung werden auch vertrauliche Metadaten mit gesichert. Hieraus ableitend bedeutet dies, die Informationen müssen auf allen Systemen und zusätzlich bei der Übermittlung geschützt werden. Zusätzlich ist sicherzustellen, dass nur Berechtigte auf die gesicherten Protokollierungsdaten zugreifen können. Es ist zu dokumentieren, welche Personen bzw. Personenkreis, in welcher Rolle Zugriff auf diese Informationen erhalten haben.

Zusätzlich sind alle administrativen Tätigkeiten an den TK-Komponenten zu protokollieren.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

### Aufstellung der TK-Anlage (NET.4.1.A7)

Am Aufstellungsort der zentralen TK-Komponenten sind mindestens dieselben Vorkehrungen getroffen worden, die an Standorten für geschäftskritische IT-Systeme realisiert sind (Unterbrechungsfreie Stromversorgung (USV), Klimatisierung, Brandschutz usw.). Eine gemeinsame Nutzung derselben Versorgungslösungen durch die zentralen TK-Komponenten und gleichzeitig durch weitere geschäftskritische IT-Systeme ist zu prüfen und zu dokumentieren.

Als Basis für die Einleitung und Koordination notwendiger Maßnahmen kommt bei Großstörungen bzw. in Notfallsituationen einer möglichst unterbrechungsfreien Verfügbarkeit der Telefonie und damit auch der zentralen TK-Anlage besondere Bedeutung zu. Um diesen Umstand gezielt Rechnung tragen zu können, sind für notfallbedingte Engpässe Pläne für die Koordinierung des Wiederanlaufs bzw. Priorisierung notwendiger Maßnahmen zu erarbeiten.

### Einschränkung und Sperrung nicht benötigter oder sicherheitskritischer Leistungsmerkmale (NET.4.1.A8)

Soweit Leistungsmerkmale nicht benötigt werden bzw. bewusst nicht verwendet werden sollen, sind diese zu sperren. Auf diese Weise ist zu verhindern, dass die Anlage über nicht benötigte Merkmale unnötig potenziellen Angriffen ausgesetzt wird. Die aufgeführten Merkmale sind hinsichtlich der zur Verfügung zustellenden Leistungsmerkmale und dem hiermit einhergehenden Missbrauchspotenzial zu bewerten.

Welches Missbrauchspotenzial besteht:

* beim direkten Ansprechen bzw. der automatischen Rufannahme in Verbindung mit der Freisprechfunktionalität des Telefons zum Abhören von Räumen,
* in öffentlichen Bereichen bei leicht zugänglichen Telefonen einem nichtkalkulierbaren Mehraufkommen an Anrufgebühren,
* bei Verwendung der Dial-In-Möglichkeiten im Endteilnehmer-Umfeld,
* bei Nutzung der Export-Merkmale hinsichtlich potenzieller Angriffe auf die Vertraulichkeit des Gesprächs?

Die Ergebnisse der Bewertung sind zu dokumentieren und die entsprechenden Sicherheitsmaßnahmen zur Reduzierung des Missbrauchspotenzials sind zu etablieren.

### Schulung zur sicheren Nutzung von TK-Anlagen (NET.4.1.A9)

Alle Benutzer der TK-Anlagen sind im Umgang mit den TK-Anlagen zu schulen. Insbesondere sind zur Erkennung der Warnanzeigen, -töne und -symbole deren Bedeutung zu vermitteln. Mindestens beinhaltet die Schulung die hier aufgeführten Symbole:

* Aufmerksamkeitston für direktes Ansprechen,
* Aufschalte-Warnton,
* Freisprechanzeige,
* Anzeige für aktiviertes direktes Ansprechen,
* Anzeige für automatischen Rückruf und
* Anzeige/Einblendung bei Dreierkonferenz.

Die Mitarbeitenden der <Institution> können je nach Benutzergruppen unterschiedlich geschult werden. Dies bedeutet, Administratoren erhalten Schulungen mit anderen Inhalten als die Benutzer. Unabhängig von der Benutzergruppe ist es wichtig in der Schulung, zusätzlich auf den Schutz der Telefone durch Passwörter/Pin hinzuweisen, um zu verhindern, dass Unberechtigte auf vertrauliche, in den Endgeräten gespeicherte Informationen zugreifen können.

Auffälliges Verhalten der Telefone oder TK-Anlage ist unverzüglich den entsprechenden Verantwortlichen über die etablierten Prozesse zu melden.

### Dokumentation und Revision der TK-Anlagenkonfiguration (NET.4.1.A10)

Die Konfigurationsdokumentation der TK-Anlagen erfolgt über idealerweise auf Basis eines einheitlichen Template für die Erstellung von Betriebshandbüchern und ist anlassbezogen fortzuschrieben. In regelmäßigen Abständen ist eine Revision der Konfiguration im Rahmen des kontinuierlichen Verbesserungsprozesses zu etablieren. Die daraus resultierenden Ergebnisse werden dem <Informationssicherheitsbeauftragter> und den Verantwortlichen für die TK-Anlage vorgelegt.

### Außerbetriebnahme von TK-Anlagen und –Geräten (NET.4.1.A11)

Die Anforderungen an die Außerbetriebnahme von TK-Anlagen und -Geräten sind entsprechend den internen Vorgaben der <Institution> abzustimmen und umzusetzen.

### Datensicherung der Konfigurationsdateien (NET.4.1.A12)

Die Konfigurations- und Anwendungsdaten der eingesetzten TK-Anlage sind regelmäßig zu sichern, insbesondere nachdem sich diese geändert haben. Dazu muss ein entsprechendes Konzept erstellt und mit den allgemeinen Konzepten der Datensicherung und deren Verantwortlichen abgestimmt sein. Aufgrund der Ähnlichkeit empfiehlt sich bei der Erstellung und Abstimmung des Konzepts, an dem für Router, Switch oder Firewalls zu orientieren.

Ebenfalls sind Anwendungsdaten wie Kontaktinformationen oder Abrechnungsdaten sichern, sofern diese von den Systemen in der Verantwortung der <Institution> erhoben werden. Sicherungszeitpunkte und Formen müssen die Anforderungen an die vertraglich vereinbarten maximal tolerablen Datenverluste berücksichtigen. Wesentlich ist, dass in jedem Fall mithilfe der getroffenen Vorkehrungen der aktuelle Zustand vor Eintreten einer Störung oder eines Notfalls wiederherstellbar ist.

### Beschaffung von TK-Anlagen (NET.4.1.A13)

Bei der Beschaffung der TK-Anlagen sollten die Ergebnisse der Anforderungsanalyse und der Planung mit einbezogen werden. Darüber hinaus sollten vorhandene Kommunikationssysteme und -komponenten bei der Beschaffung berücksichtigt werden.

### Notfallfürsorge für TK-Anlagen (NET.4.1.A14)

Grundlage eines sicheren Betriebs der TK-Anlagen ist die Vorbereitung auf Störungssituationen. Hierzu gehören Ausfälle oder Beeinträchtigungen von Hardware und Software aufgrund von Defekten oder Kompromittierung. Für typische und für bereits aufgetretene Schadenssituationen werden Sofortmaßnahmen und weiterführende Handlungsanweisungen erstellt. Es ist zu überprüfen, ob ein separater PSTN-Anschluss für Katastrophenschaltungen bereitzuhalten ist, um Notrufe absetzten zu können.

Für die TK-Anlagen in der Verantwortlichkeit der <Institution> sind Notfallpläne unter Einbindung der betroffenen Parteien zu erstellen und in das Notfallkonzept der <Institution> zu integrieren. Durch regelmäßige Notfallübungen sind die etablierten Notfallpläne praktisch zu verifizieren.

### Notrufe bei einem Ausfall der TK-Anlage (NET.4.1.A15)

Es ist sicherzustellen, dass auch bei einem Ausfall der TK-Anlagen Location-based Notrufe (LBS) aus den Räumlichkeiten der <Institution> abgesetzt werden können.

Bei Ausfällen im Bereich der zentralen TK-Anlage kann nicht sichergestellt werden, ob an dieser Anlage angeschlossene Telefone noch Notrufe absetzen können. Als Ausweichlösung ist zu prüfen, ob hier ein separater PSTN-Anschluss mit direkt angebundenem Telefon eingesetzt werden kann. Sofern ein separater PSTN-Anschluss mit direkt angebundenem Telefon bereitgestellt wird, ist darauf zu achten, dass entsprechend der räumlichen Ausdehnung diese Telefone geeignet platziert werden und eine angemessene Anzahl vorhanden ist.

### Sicherung von Telefonie-Endgeräten in frei zugänglichen Räumen (NET.4.1.A16)

Der Funktionsumfang der Telefonie-Endgeräte ist in frei zugänglichen Räumen einzuschränken. Endgeräte, bei denen die Einschränkung nicht möglich ist, sind geeignet vor unbefugtem Zugriff geschützt.

### Wartung von TK-Anlagen (NET.4.1.A17)

Die Geräte zur Wartung und Konfiguration der TK-Anlage werden mit Passwörtern bzw. PINs abgesichert. Die Datenverbindung bei IP-basierten Zugängen zur TK-Anlage sind verschlüsseln.

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Erhöhter Zugriffsschutz (NET.4.1.A18 - CA)

Die TK-Anlagen in der Verantwortung der <Institution> sind sofern lokal am Standort betrieben in einem separaten sowie geeignet gesicherten Raum aufzustellen. Nur ein eingeschränkter Personenkreis darf Zutritt, Zugang und Zugriff zur TK-Anlage erhalten.

### Redundanter Anschluss (NET.4.1.A19 - A)

Der Anschluss an die TK-Anlage und deren zentralen Servicekomponenten sollten redundant ausgelegt werden.