Bundesamt
für Sicherheit in der
Informationstechnik

NET.4.1 TK-Anlagen

1. Beschreibung

1.1. Einleitung

Mit einer Telekommunikationsanlage, kurz TK-Anlage, können die Telefone einer 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 Bewegtbilder zu übertragen. Die Informationen können dabei analog oder digital über drahtgebundene oder drahtlose Übertragungsmedien weitergeleitet werden. Je nach Anbindung und genutzten Datennetzen können in einer Institution verschiedenste Telekommunikationsanlagen eingesetzt werden.

1.2. Zielsetzung

In diesem Baustein werden die für die TK-Anlagen sowie die entsprechenden Anteile von Hybrid-Anlagen spezifischen Gefährdungen und Anforderungen betrachtet. Das Ziel des Bausteins ist der Schutz der Informationen, die über TK-Anlagen übermittelt werden sowie der Schutz der Anlage vor Fremdeingriffen und Manipulationen.

1.3. Abgrenzung und Modellierung

Der Baustein NET.4.1 *TK-Anlagen* ist auf jede TK-Anlage anzuwenden.

Dieser Baustein behandelt die Gefährdungen und Anforderungen, die spezifisch für eine TK-Anlage sowie die entsprechenden Teile einer Hybrid-Anlage sind. Themen, die über die TK-Anlage hinausgehen, wie zum Beispiel Gefährdungen und Anforderungen für einzelne VoIP-Implementierungen, sowie extern bereitgestellte Dienste werden in den entsprechenden Bausteinen des IT-Grundschutz-Kompendiums gesondert behandelt.

Die Sicherheitsaspekte von VoIP-Komponenten und der Sprachübertragung über VoIP werden im Baustein NET.4.2 *VoIP* näher betrachtet.

TK-Anlagen sollten grundsätzlich mit berücksichtigt werden, wenn die Bausteine ORP.4 *Identitäts- und Berechtigungsmanagemen*t, OPS.1.2.5 *Fernwartung*, CON.3 *Datensicherungskonzept* und OPS.1.1.5 *Protokollierung* umgesetzt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.4.1 *TK-Anlagen* von besonderer Bedeutung.

2.1. Abhören von TK-Anlagen

Wenn Telefongespräche oder Daten über eine TK-Anlage unverschlüsselt übertragen werden, besteht grundsätzlich die Gefahr, dass Angreifende Informationen mithören oder mitlesen. So könnten sie beispielsweise die Telefonkabel direkt anzapfen oder an einer zwischen den Gesprächsteilnehmenden vermittelnden TK-Anlage lauschen.

Bei vielen TK-Anlagen können Anrufende Empfangenden Nachrichten hinterlassen, wenn diese zum Zeitpunkt des Anrufs telefonisch nicht erreichbar sind. Einige Anrufbeantworter, vor allem bei VoIP-Anlagen, verschicken diese Informationen als Audio-Datei in einer E-Mail. Der Inhalt dieser E-Mail könnte direkt von Angreifenden abgefangen und angehört werden.

Des Weiteren könnten Gespräche durch das Aktivieren von gesperrten, in Deutschland zum Teil unzulässigen, Leistungsmerkmalen von Dritten mitgehört werden. Ein Beispiel hierfür ist die Zeugenschaltung. Eine derartige Aktivierung erfordert zwar genauere Systemkenntnisse, ist aber aufgrund vieler frei verfügbarer Hinweise im Internet häufig kein großes Hindernis.

2.2. Abhören von Räumen über TK-Anlagen

Über Mikrofone in Endgeräten können grundsätzlich auch Räume abgehört werden. Dabei werden zwei Varianten unterschieden:

Bei der ersten Variante können Endgeräte, wenn entsprechende Funktionen implementiert sind, aus dem öffentlichen Netz oder über das LAN dazu veranlasst werden, die eingebauten Mikrofone zu aktivieren. Ein bekanntes Beispiel hierfür ist die sogenannte „Baby-Watch-Funktion“ von Telefonen oder Anrufbeantwortern.

Bei der zweiten Variante kann das Leistungsmerkmal „direktes Ansprechen“ in Kombination mit der Option „Freisprechen“ missbraucht werden. Die auf diese Weise realisierbare Funktion einer Wechselsprechanlage kann unter gewissen Umständen auch zum Abhören eines Raumes ausgenutzt werden.

2.3. Gebührenbetrug

Gebührenbetrug im Zusammenhang mit Daten- oder Telekommunikationsdiensten hat das Ziel, die Kosten für geführte Telefonate oder Datentransfers auf Dritte zu übertragen. Eine TK-Anlage lässt sich auf verschiedene Weise von außen manipulieren. Zum einen können Angreifende versuchen, vorhandene Leistungsmerkmale für den Gebührenbetrug zu missbrauchen. Zu diesen Leistungsmerkmalen zählen beispielsweise aus der Ferne umprogrammierbare Rufumleitungen oder Dial-in-Optionen. Zum anderen können die Berechtigungen so vergeben werden, dass kommende „Amtsleitungen“ abgehende „Amtsleitungen“ belegen. Auf diese Weise können Anrufenden bei Anwahl einer bestimmten Rufnummer auf Kosten des TK-Anlagenbetreibenden von außen automatisch wieder mit dem „Amt“ verbunden werden.

Darüber hinaus können nicht nur Angreifende von außen, sondern auch die Beschäftigten innerhalb einer Institution mit den Gebühren betrügen. So können sie etwa versuchen, auf Kosten der Institution oder der anderen Beschäftigten zu telefonieren, indem sie z. B. von fremden Apparaten telefonieren, fremde Berechtigungscodes (Passwörter) auslesen oder persönliche Berechtigungen verändern.

2.4. Missbrauch frei zugänglicher Telefonanschlüsse

Oft werden Telefone betrieben, die keinen Benutzenden persönlich zugeordnet sind. Einige dieser Telefone, wie zum Beispiel solche in Druckerräumen, sind nur einem eingeschränkten Personenkreis zugänglich. Andererseits sind Telefone häufig in Bereichen zu finden, die für Besuchende frei zugänglich sind. Dazu zählen beispielsweise Parkhäuser oder Bereiche vor Zugangskontrollsystemen. Besitzen diese Telefone ein elektronisches Telefonbuch, in dem interne Telefonnummern gespeichert sind, könnten diese Nummern ungewollt nach außen gelangen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.4.1 *TK-Anlagen* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Fachverantwortliche
Weitere Zuständigkeiten	IT-Betrieb, Vorgesetzte

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

NET.4.1.A1 Anforderungsanalyse und Planung für TK-Anlagen (B) [IT-Betrieb]

Vor der Beschaffung oder Erweiterung einer TK-Anlage MUSS eine Anforderungsanalyse durchgeführt werden. Im Rahmen dieser Analyse MUSS festgelegt werden, welche Funktionen die TK-Anlage bieten soll. Hierbei MÜSSEN neben der Ausprägung der TK-Anlage auch die Anzahl der benötigten Verbindungen und Anschlüsse festgelegt werden. Auch eine mögliche Erweiterbarkeit und grundlegenden Sicherheitsfunktionen MÜSSEN bei der Planung betrachtet werden. Darüber hinaus MÜSSEN je nach Bedarf Support- und Wartungsverträge für die TK-Anlage berücksichtigt werden. Basierend auf den ermittelten Anforderungen MUSS anschließend der Einsatz der TK-Anlage geplant und dokumentiert werden. Die zuvor ermittelten Anforderungen und die Planung MÜSSEN mit den entsprechenden IT-Zuständigen abgestimmt werden.

NET.4.1.A2 Auswahl von TK-Diensteanbietenden (B) [IT-Betrieb]

Um mit Personen telefonieren zu können, deren Telefone nicht an die institutionseigene TK-Anlage angeschlossen sind, MUSS ein TK-Diensteanbieter oder TK-Diensteanbieterin beauftragt werden. Dabei MÜSSEN die Anforderungen an die TK-Anlage, die Sicherheitsrichtlinie sowie vertragliche und finanzielle Aspekte berücksichtigt werden. Alle vereinbarten Leistungen MÜSSEN eindeutig schriftlich festgehalten werden.

NET.4.1.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.4.1.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

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

Bei TK-Anlagen MÜSSEN geeignete Daten erfasst und bei Bedarf ausgewertet werden. Protokolliert werden MÜSSEN zusätzlich alle systemtechnischen Eingriffe, die Programmveränderungen beinhalten, sowie Auswertungsläufe, Datenübermittlungen und Datenzugriffe. Alle Administrationsarbeiten an der TK-Anlage MÜSSEN ebenfalls protokolliert werden. Die protokollierten Informationen SOLLTEN regelmäßig kontrolliert werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

NET.4.1.A6 Erstellung einer Sicherheitsrichtlinie für TK-Anlagen (S) [IT-Betrieb]

Basierend auf der institutionsweiten Sicherheitsrichtlinie SOLLTE eine eigene Sicherheitsrichtlinie für die TK-Anlage erstellt werden. Diese Sicherheitsrichtlinie für die TK-Anlage SOLLTE grundlegende Aussagen zur Vertraulichkeit, Verfügbarkeit und Integrität beinhalten. Sie SOLLTE allen Personen, die an der Beschaffung, dem Aufbau, der Umsetzung und dem Betrieb der TK-Anlage beteiligt sind, bekannt sein und die Grundlage für deren Arbeit darstellen. Die zentralen sicherheitstechnischen Anforderungen an die TK-Anlage sowie das zu erreichende Sicherheitsniveau SOLLTEN in der institutionsweite Sicherheitsrichtlinie aufgenommen werden.

NET.4.1.A7 Geeignete Aufstellung der TK-Anlage (S)

Die TK-Anlage SOLLTE in einem geeigneten Raum untergebracht sein. Die Schnittstellen an der TK-Anlage, besonders nicht genutzte Schnittstellen, SOLLTEN geeignet geschützt werden.

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

Der Umfang der verfügbaren Leistungsmerkmale SOLLTE auf das notwendige Minimum beschränkt werden. Nur die benötigten Leistungsmerkmale SOLLTEN freigeschaltet werden. Die nicht benötigten oder wegen ihres Missbrauchspotenzials als kritisch eingestuften Leistungsmerkmale SOLLTEN so weit wie möglich an der zentralen Anlage abgeschaltet werden. Zusätzliche Schutzmaßnahmen SOLLTEN für die auf den Endgeräten gespeicherten und abrufbaren vertraulichen Daten ergriffen werden.

NET.4.1.A9 Schulung zur sicheren Nutzung von TK-Anlagen (S) [Vorgesetzte]

Die Benutzenden der TK-Anlage SOLLTEN in die korrekte Verwendung von Diensten und Geräten eingewiesen werden. Den Benutzenden der TK-Anlage SOLLTEN alle notwendigen Unterlagen zur Bedienung der entsprechenden Endgeräte zur Verfügung gestellt werden. Sämtliche Auffälligkeiten und Unregelmäßigkeiten der TK-Anlage SOLLTEN den entsprechenden Verantwortlichen gemeldet werden.

NET.4.1.A10 Dokumentation und Revision der TK-Anlagenkonfiguration (S) [IT-Betrieb]

Die TK-Anlagenkonfiguration SOLLTE geeignet dokumentiert und fortgeschrieben werden. Die TK-Anlagenkonfiguration SOLLTE in regelmäßigen Abständen überprüft werden. Das Ergebnis der

Prüfung SOLLTE zumindest den Informationssicherheitsbeauftragten, den Fachverantwortlichen und anderen verantwortlichen Mitarbeitenden vorgelegt werden.

NET.4.1.A11 Außerbetriebnahme von TK-Anlagen und -geräten (S) [IT-Betrieb]

Die Aussonderung von TK-Anlagen und angeschlossenen TK-Geräten SOLLTE in der Sicherheitsrichtlinie berücksichtigt werden. Alle Daten, die auf TK-Anlagen oder Endgeräten gespeichert sind, SOLLTEN vor der Aussonderung sicher gelöscht werden.

NET.4.1.A12 Datensicherung der Konfigurationsdateien (S)

Die Konfigurations- und Anwendungsdaten der eingesetzten TK-Anlage SOLLTEN bei der Ersteinrichtung und anschließend regelmäßig gesichert werden, insbesondere nachdem sich diese geändert haben. Es SOLLTE regelmäßig geprüft und dokumentiert werden, ob die Sicherungen der TK-Anlagen auch tatsächlich als Basis für eine Systemwiederherstellung genutzt werden können.

Es SOLLTE ein Datensicherungskonzept für TK-Anlagen erstellt und mit den allgemeinen Konzepten der Datensicherung für Server und Netzkomponenten abgestimmt werden.

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

Bei der Beschaffung von TK-Anlagen SOLLTEN die Ergebnisse der Anforderungsanalyse und der Planung miteinbezogen werden. Bei der Beschaffung einer TK-Anlage SOLLTE beachtet werden, dass sie neben digitalen auch analoge Teilnehmeranschlüsse anbieten sollte. Darüber hinaus SOLLTEN vorhandene Kommunikationssysteme und -komponenten bei der Beschaffung berücksichtigt werden.

NET.4.1.A14 Notfallvorsorge für TK-Anlagen (S)

Es SOLLTE ein Notfallplan für die TK-Anlage erstellt werden. Dieser SOLLTE in das Notfallkonzept der Institution integriert werden. Es SOLLTEN regelmäßig Notfallübungen bezüglich der TK-Anlagen durchgeführt werden.

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

Es SOLLTE sichergestellt werden, dass auch bei einem Ausfall der TK-Anlage Notrufe aus der Institution abgesetzt werden können. Die Notrufmöglichkeiten SOLLTEN von allen Räumen aus auf ausreichend kurzen Wegen erreichbar sein.

NET.4.1.A16 Sicherung von Endgeräten in frei zugänglichen Räumen (S)

Der Funktionsumfang der Endgeräte, die in frei zugänglichen Räumen aufgestellt werden sollen, SOLLTE eingeschränkt werden. Ist dies nicht möglich, SOLLTE das Endgerät in geeigneter Weise vor unbefugtem Zugriff geschützt werden.

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

Die Geräte zur Wartung und Konfiguration der TK-Anlage SOLLTEN mit Passwörtern bzw. PINs abgesichert sein.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

NET.4.1.A18 Erhöhter Zugangsschutz (H)

Die TK-Anlage SOLLTE in einem separaten sowie geeignet gesicherten Raum untergebracht sein. Der Zutritt und Zugang zur TK-Anlage SOLLTE nur einem eingeschränkten Personenkreis möglich sein. Externe SOLLTEN NUR beaufsichtigt Zugang zur Anlage erhalten.

NET.4.1.A19 Redundanter Anschluss (H)

Der Anschluss der TK-Anlage SOLLTE redundant ausgelegt sein. Bei IP-basierten TK-Anlagen SOLLTE ein zusätzlicher PSTN-Anschluss vorhanden sein.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat im Rahmen der Technischen Leitlinien die „BSI-TL-02013 für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf“ veröffentlicht.