Leitfaden
zur Erstellung einer betriebsinternen
Telefonanweisung (Festnetz)

A: Allgemeines

Wer kennt nicht diese Situation, Sie sitzen in der Bahn oder im Bus, beim Arzt im Wartezimmer, im Restaurant; stehen in einem Geschäft oder gehen über die Straße oder anderswo und jemand unterhält sich lautstark mit einem Telefon (Handy) und nimmt nicht mehr wahr, dass alle Umherstehenden mitbekommen, wie schlecht es der Oma geht usw...
„Solche oder noch sensiblere Themen sollte man doch lieber in den eigenen vier Wänden am Festnetztelefon erörtern, das ist doch viel sicherer“, werden viele jetzt sagen. Aber ist das Festnetztelefon wirklich sicher?
Diese Rahmenvorschrift soll ein Leitfaden sein zur Beurteilung ihrer modernen betrieblichen Telekommunikationsanlage (TK-Anlage) im Hinblick auf den Schutz von VS; ihnen und ihren Mitarbeitern/Innen aber auch Anregungen und Denkanstöße vermitteln zum Thema Vertraulichkeit Ihrer Telefongespräche. Die verwandten Themen wie Gebührenbetrug, Konkurrenzausspähung oder Sabotage werden hier nicht speziell behandelt.

1. Digitale Technik

Mit der Ablösung der analogen Technik im Bereich privater TK-Anlagen durch die Digitaltechnik sowie durch die zunehmende Verbreitung intelligenter Endgeräte ist weitgehend unbemerkt eine veränderte Gefährdungslage entstanden.
Während bei der Analogtechnik in erster Linie die Hardware des Systems (z.B. Leitungsnetz und Endgeräte) als Angriffspunkte für illegales Abhören gesehen werden mussten, steht bei digitalen Systemen die missbräuchliche Verwendung vorhandener Funktionalitäten im Vordergrund.
Ihr modernes Telefon auf ihrem Schreibtisch ist auch die ideale „Wanze“ zum Mithören aller Ihrer Gespräche – es ist unauffällig, es besitzt ein Mikrofon, es besitzt Energie (Strom) und es ist über die Telefonleitung mit der ganzen Welt verbunden.
Damit dieses Telefon nicht als „Wanze“ missbraucht werden kann, müssen entsprechende Vorkehrungen geschaffen werden.

2. Schutzmaßnahme Konfiguration

Moderne digitale TK-Anlagen enthalten optional mehrere hundert Leistungsmerkmale. Viele von Ihnen kennen und nutzen die geläufigsten Merkmale wie z.B. Freisprechen (Führen eines Telefonates ohne Abheben des Hörers), Konferenz (Führen eines Telefonates zwischen drei Personen gleichzeitig) oder Makeln (Führen von zwei gleichzeitigen Telefonaten im Wechsel).
Ein Missbrauch dieser Merkmale kann eine ungewünschte Raumüberwachung ermöglichen.
Daher ist die ordnungsgemäßen Konfiguration der TK-Anlage und ihrer umfangreichen Sicherheitsmechanismen von größter Bedeutung.
Die meisten Unternehmen lassen die Installation und Konfiguration ihrer TK-Anlage von ei-

ner Fremdfirma durchführen. Dabei ist die Auswahl einer Firma Ihres Vertrauens besonders wichtig, da Sie die Einstellungen Ihrer TK-Anlage aus der Hand geben. Sie sollten sich zumindest von dieser Fremdfirma genau erklären und demonstrieren lassen, wie die Leistungsmerkmale und Sicherheitsmechanismen geschaltet sind. Dies sollte auch in einer Beschreibung der Anlage (nicht nur Bedienungsanleitung) festgehalten werden und ihre Mitarbeiter/Innen sollten über die Nutzung der TK-Anlage geschult sein, hier sollte insbesondere auch auf mögliche Warnanzeigen, -symbole und -töne eingegangen werden. Im Alltagsbetrieb nicht benötigte Leistungsmerkmale werden deaktiviert.
In vielen Fällen kann sogar die Geheimschutzbetreuung dieser Fremdfirma erforderlich sein.

3. Schutzmaßnahme Zugriff

Der Zugriff auf TK-Anlagen kann über die Administrationsschnittstelle des zu Ihrer TK-Anlage gehörenden Rechners (Wartungs-, Diagnose- und Steuereinheit) oder über die Fernwartung (siehe Nr. 5) erfolgen. In diesem Rechner werden die Leistungsmerkmale und die Sicherheitsmechanismen für Ihre TK-Anlage ein- oder ausgeschaltet. Manipulationen an den TK-Anlagen selbst und ihren Komponenten sollen verhindert werden.
Der Raum, in denen dieser Rechner steht, aber auch alle Haupt- und Zwischenverteilerkästen sind gegen unbefugtes Öffnen zu schützen.
Sämtliche zur TK-Anlage gehörenden Kabel und Leitungen sind möglichst zugriffssicher zu verlegen.
Lagehinweise auf schützenswerte Gebäudeteile sind zu vermeiden.
Haben Fremdpersonen Zugriff auf Rechner, Verteilerkästen und Leitungen, sollten sie begleitet werden.
Der Zutritt zum Raum des Rechners der TK-Anlage sowie der Zugriff auf Verteilerkästen sind zu regeln und zu kontrollieren.
Bedienplätze größerer TK-Anlagen sind zugriffssicher unterzubringen und der Zugang ebenfalls entsprechend zu regeln.
Die Abläufe von Wartungs- und Reparaturarbeiten sind genau zu regeln.
Alle Administrationsarbeiten an der TK-Anlage sind genauestens zu protokollieren.
Zusätzlich sind die Regeln des Passwortschutzes einzuhalten.

4. Fernwartung

Aus Gründen der Wirtschaftlichkeit und der Verfügbarkeit der Anlage wird gern auf den Fernwartungsservice der Hersteller zurückgegriffen. Da der Wartungsport Ihrer TK-Anlage dafür amtsberechtigt sein muss, kann er ohne zusätzliche Maßnahmen weltweit angewählt werden. Die möglichen Schutzmaßnahmen um nachzuvollziehen, wer wann welche Änderungen vorgenommen hat (z.B. automatischer Rückruf, Auswertung der im ISDN übermittelten Rufnummern, Sperrung des Fernwartungszuganges im Normalfall und Aktivierung nur auf spezielle Nachfrage, lückenlose Protokollierung aller Administrationstätigkeiten), können jedoch nicht gegenüber den unter Nummer 3. genannten Schutzmaßnahmen als gleichwertig angesehen werden.

5. Schutzmaßnahme Vertraulichkeit

Die Kommunikation über elektronische Medien ist für unsere Gesellschaft unverzichtbar geworden. Einrichtungen wie Telefon, Telefax, lokale Netze, Datenfernübertragung, E-Mail sind für ein effizientes Arbeiten nicht mehr wegzudenken; die Zeit der "reitenden Boten" ist längst vorbei.
Fast allen elektronischen Informations-Übertragungsverfahren ist gemeinsam, dass der In-

formationsfluss über Leitungen erfolgt. Ob es sich hierbei um Koaxial-, Zweidraht-, Twisted-Pair- oder Glasfaser-Leitungen handelt, bleibt dem Anwender meistens verborgen, sofern nur die Übertragung einwandfrei funktioniert. Dazu gehört auch, dass ca. 50 % aller Telefonverbindungen im Laufe ihrer Strecke teilweise über eine Richtfunkstrecke geführt werden und somit von entsprechenden Empfangseinrichtungen mitgehört werden.
Ebenso verborgen bleibt dem Anwender vielfach die Tatsache, dass auf Leitungen übertragene elektrische Signale auf andere Leitungen überkoppeln (Frequenzen auf der einen Leitung werden auf andere Leitungen übertragen bei schlechter Isolierung der Leitungen) können und damit ein Verlust der Vertraulichkeit droht.
Dabei ist der physikalische Effekt, dass elektrische Signale auf benachbart verlegte Leitungen überkoppeln, vielen aus eigener Erfahrung unbewusst bekannt. Beim Telefonieren mit herkömmlichen, analog arbeitenden Telefonapparaten hört man mitunter leise Stimmen im Hintergrund, die nicht dem angewählten Gesprächspartner zuzuordnen sind. Wer hier eine Fehlschaltung irgendwo auf dem langen Übertragungsweg vermutet, denkt nicht an das Nächstliegende, dass nämlich beispielsweise ein Nachbar, dessen Telefonleitung im selben Kabelbündel wie das eigene geführt ist, ebenfalls telefoniert. Dass ein einigermaßen versierter Elektronikbastler in der Lage ist, das "übergekoppelte" Gespräch mit geringem Aufwand aufzubereiten und so einwandfrei mithörbar zu machen, ist fast selbstverständlich.

Schutzmaßnahmen gegen Verlust der Vertraulichkeit lassen sich aus den physikalischen Effekten folgern, die zum Überkoppeln auf Leitungen führen.

Geeignete Schutzmaßnahmen sind:

- Verwendung von Kabeltypen, deren Aufbau so gestaltet ist, dass nur ein geringes elektromagnetisches Feld freigesetzt wird, z.B. Koaxial- oder Twisted-Pair-Kabel.

- Verwendung von Kabeltypen mit hochwertiger, vorzugsweise doppelter Schirmung. Als sehr wirksam und kostengünstig hat sich eine Kombination aus Folien- und Geflechtschirm erwiesen.

- Verlegung der bedrohten Leitungen mit ausreichendem Abstand zu anderen, parallel geführten Leitungen (Von einem Arbeitsplatzcomputer werden Informationen beispielsweise zu einem Hostrechner oder Netzserver übertragen. Die Übertragungsleitung befindet sich in einem vor Zugriff durch Unbefugte gesicherten Bereich, ist jedoch zusammen mit anderen Leitungen im selben Kabelkanal verlegt. Eine der anderen Leitungen, beispielsweise eine Telefonleitung, verlässt den gesicherten Bereich. Dort ist es mit verhältnismäßig geringem Aufwand möglich, das übergekoppelte Informationssignal von der Leitung abzugreifen, aufzubereiten und darzustellen bzw. für eine spätere Auswertung zu speichern. Bezüglich digitaler, auf Leitungen übertragener Signale (z.B. ISDN) ist anzumerken, dass die von einer parallel verlegten Leitung übergekoppelte Signalamplitude meist so gering ist, dass die eigentliche Funktion der Leitungen nicht beeinträchtigt wird und so das Überkoppeln von den Nutzern dieser Leitungen nicht bemerkt wird. Erst eine geeignete Aufbereitung des übergekoppelten Signals erlaubt eine Rekonstruktion der Information).

- Verringerung des Signal-Oberwellengehalts durch elektrische Filterung bei digitaler Übertragung von Informationen.
  Die Oberwellen, für deren Intensität die Flankensteilheit des digitalen Signals ein Maß ist, sind für die eigentliche Informationsübertragung nicht notwendig, koppeln aber

besonders stark auf parallel geführte Leitungen über.

- Verwendung von Lichtwellenleiterkabeln (Glas- oder Kunststofffasern). Lichtwellenleiter erzeugen kein elektromagnetisches Feld, können jedoch unter Umständen optisch überkoppeln, wenn sich zwischen den einzelnen Fasern keine optisch undurchlässige Ummantelung befindet.

B: Verbindliche Regelungen zum Schutz von VS-Gesprächen

Bedingt durch die Möglichkeit der Manipulation von TK-Anlagen und der Gefährdungen durch die Übertragung auf Telekommunikationswegen einschließlich Überkoppeln gilt für die Übermittlung von staatlichen Verschlusssachen:

- keine nicht den Vorgaben des BMWi entsprechend verschlüsselte Telefongespräche
- keine nicht den Vorgaben des BMWi entsprechend verschlüsselte Faxe
- keine nicht den Vorgaben des BMWi entsprechend verschlüsselte Emails
- keine nicht den Vorgaben des BMWi entsprechend verschlüsselte Datenübertragungen.

Ist in Ihrem Unternehmen eine Besprechung (auch unter Mitarbeitern im kleinen Kreise) über VS-eingestufte Inhalte geplant, so sind vorhandene Telefonapparate durch Entfernung des Leitungssteckers vom Netz zu trennen. Sollte dies aus technischen Gründen nicht möglich sein, sind vorhandene Telefonapparate von der Zentrale aus zu deaktivieren oder andere gleichwertige Maßnahmen vorzusehen.

Bei Unternehmen mit größerem VS-Bestand, Sperr- und Kontrollzonen oder häufig stattfindenden Besprechungen mit VS-Inhalten ist eine Fernwartung nicht zulässig.
Hier ist mit Einwilligung des BMWi das Personal, dass die Installation, Instandsetzung, Wartung und Betrieb der TK-Anlage und aller ihrer Komponenten durchführt, entsprechend der vorhandenen VS sicherheitsmäßig zu überprüfen und zum Zugang zu VS zu ermächtigen. Werden diese Aufgaben nicht von eigenem Personal durchgeführt, können andere Firmen hierzu auch in die Geheimschutzbetreuung des BMWi aufgenommen werden.

Die weiteren unter Abschnitt A Nr. 3 „Schutzmaßnahmen Zugriff“ enthaltenen allgemeinen Empfehlungen sind für den Schutz von staatlichen VS zu beachten und hier verbindlich. Sollte eine dieser Forderungen nicht erfüllt werden können, ist in Abstimmung mit dem BMWi ein gleichwertiger Schutz sicherzustellen (z.B. sind vorhandene bauliche Kabelführungen nicht zugriffssicher verlegt, so müssen sie in offen zugänglichen Bereichen auf Unversehrtheit in regelmäßigen Abständen geprüft werden. Nicht offen zugängliche Bereiche sind dabei unter Verschluss des SiBe oder einer von ihm beauftragten Person zu halten).