Erläuterung der neuen Richtlinien des BAKOM zur Sicherheit und Verfügbarkeit von Fernmeldeinfrastrukturen und -diensten

Als Grundlage für das Konzept dieser Richtlinien dienen die Grundsätze des Management der Informationssicherheit, auf denen die bedeutenden Normen basieren.

An erster Stelle wird in den Richtlinien den Fernmeldedienstanbieterinnen (FDA) empfohlen, eine Sicherheitspolitik festzulegen und zu verfolgen, auf der das Management der Informationssicherheit aufbaut. Ihr Ziel besteht darin, wichtige und sensible Ressourcen innerhalb der Organisation zu wahren und zu sichern. Sie beschreibt vor allem den Standpunkt der Unternehmensleitung in Bezug auf die Sicherheit und definiert auf Grund der Gefahrenquellen der Umfang der Sicherheit.An zweiter Stelle werden die FDA aufgefordert, ein Information Security Management System (ISMS) gemäss den Anforderungen der Empfehlung X.1051 zu implementieren. Diese Empfehlung wurde ausgearbeitet, damit FDA beweisen können, dass die Sicherheit gewährleistet ist. Dadurch wird das Vertrauen der Teilnehmer in ihre Praktiken gefördert. Diese Empfehlung verfolgt das gleiche Ziel wie unsere Richtlinien. Sie überträgt nämlich die Grundsätze der Norm BS 7799-2 (specification for information security management systems) auf den Bereich der modernen Telekommunikation.

Dieses Dokument beschreibt einen Prozess der kontinuierlichen Verbesserung durch das Durchlaufen der vier Phasen „PLAN-DO-CHECK-ACT“. Diese Abfolge wird in der Norm BS 7799-2, aber auch in anderen Management-Systemen genannt, z. B. in den Normen ISO 9001 für das Qualitätsmanagement oder ISO 14001 im Umweltbereich. Das Vier-Phasen-Modell widerspiegelt im Übrigen die Grundsätze der OECD-Richtlinie über die Sicherheit von Informationssystemen und Netzen (2002 OECD Guidance on the Security of Information Systems and Networks).

In der Planungsphase (PLAN) sind Ziele zu definieren. Die FDA sollte insbesondere die Risiken identifizieren und einschätzen, und danach entsprechende Kontrollziele bestimmen. In der darauf folgenden Durchführungsphase (DO) werden Verfahren und Kontrollen durchgeführt, um die definierten Ziele zu erreichen.

Danach folgt eine Phase der Beurteilung und Überprüfung des ISMS (CHECK), um die Wirksamkeit des Systems einzuschätzen, das Ausmass des Restrisikos zu bewerten und die Auswirkungen bestimmter Ereignisse auf die Informationssicherheit zu berücksichtigen.

Die letzte Phase (ACT) fordert die FDA auf, das ISMS regelmässig zu verbessern.

Wie von den Normen BS 7799-2 und ISO 9001 wird eine Dokumentierung des ISMS verlangt. Diese könnte als Grundlage für allfällige Aufsichtstätigkeiten des BAKOM dienen.

An dritter Stelle – nach der Empfehlung, ein ISMS aufzubauen – wird in den Richtlinien auf die Dokumente ITU-T X.1051, ITU-T E.408 und ISO 17799 für die Durchführung von Verfahren und Kontrollen im Rahmen des ISMS verwiesen. Die konsultierten FDA haben sich einhellig für solche Verweise ausgesprochen; der Publikation eines neuen Dokuments zu diesem Thema ziehen sie die Verwendung der Norm ISO 17799 vor, an der sie sich bereits orientieren. Dieses Dokument, das als „Best Practice Code“ bezeichnet wird, ist eigentlich eine detaillierte und kommentierte Liste von Sicherheitsmassnahmen, die eine einheitliche Auslegung fördert.

Es scheint uns sinnvoll zu sein, in den Richtlinien auf die relativ neuen Dokumente X.1051 und E.408 der ITU-T zu verweisen, da dieses Gremium für Telekommunikationsstandardisierung vorsieht, sich bei der Ausarbeitung eines künftigen Dokuments über Netzsicherheit auf diese Publikationen zu stützen (ITU-T Study Group 17, TD 2048 Rev. 3, Proposal for a new Project – Security baseline for Network Operators).

Zusätzlich wird den FDA in den Richtlinien empfohlen, eine Kontinuitätsplanung (Business Continuity Plan) und eine Planung der Betriebswiederherstellung nach einer Katastrophe (Disaster Recovery Plan) zu erstellen, die grundsätzlich ebenfalls zum Sicherheitsmanagement-Prinzip gehören.

Ziel der Kontinuitätsplanung ist, bei einer Panne so zu reagieren, dass ihre Folgen möglichst gering sind. Die Planung der Betriebswiederherstellung beschreibt hingegen, welche Verfahren zu befolgen sind, um zum normalen Betrieb zurückzukehren.

Schliesslich wird in den Richtlinien den FDA empfohlen, eigene Verfahren und eine eigene Infrastruktur aufzubauen, die den anerkannten Standards im Bereich der Informations- und Infrastruktursicherheit entsprechen. Angesichts der wichtigen Entwicklungen, die innerhalb der verschiedenen Standardisierungsgremien festzustellen sind, könnte das BAKOM in Zukunft eine Liste der Referenzdokumente als Anhang zu den Richtlinien publizieren und unterhalten.

14.11.05/BAKOM/jec