Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Kommunikation BAKOM
Abteilung Telecomdienste

Ausgabe 3, Mai 2009

Richtlinien zur Sicherheit und Verfügbarkeit von Fernmeldeinfrastrukturen und -diensten

Inhaltsverzeichnis

1 Allgemeines

1.1 Geltungsbereich

Das Fernmeldegesetz (FMG) [1] hat u.a. zum Ziel, dass der Bevölkerung und der Wirtschaft qualitativ hoch stehende Fernmeldedienste angeboten werden und ein störungsfreier Fernmeldeverkehr gewährleistet ist (Art. 1 FMG [1]). Die Telekommunikation basiert definitionsgemäss auf miteinander kommunizierenden Teilnetzen, die einander beeinflussen und voneinander abhängig sind. Es ist deshalb wichtig, über ein gemeinsames Verständnis des minimalen Standards an Sicherheit zu verfügen. Die Telekommunikationsnetze und -dienste sind letztlich nur so sicher und verfügbar wie das schwächste Glied des Ganzen.

Zweck dieser Richtlinien zur Sicherheit und Verfügbarkeit von Fernmeldeinfrastrukturen und -diensten ist die Präzisierung der Sicherheitsanforderungen des Gesetzgebers, damit die betroffenen Kreise diese einheitlich auslegen und das Konsumentenvertrauen gestärkt wird. Zudem definieren diese Richtlinien ein Mindestsicherheitsniveau, das jede Fernmeldedienstanbieterin gewährleisten sollte, um zur Zuverlässigkeit und Verfügbarkeit des gesamten nationalen Fernmeldewesens beizutragen.

Diese Richtlinien haben Empfehlungsstatus und gelten für öffentliche Fest- und Funknetze, mit denen in gewöhnlichen Situationen Sprach- und Datendienste hergestellt werden. Die Richtlinien können zudem im Zusammenhang mit der Bestimmung zur Sicherheit und Verfügbarkeit in Art. 48a FMG [1] gesehen werden.

1.2 Stellenwert dieser Richtlinien

Das Bundesamt für Kommunikation (BAKOM) hat sich bei der Ausarbeitung dieses Dokuments auf die Arbeiten der Standardisierungsgremien und auf die Ergebnisse einer Konsultation der betroffenen Kreise gestützt.

Dieses Dokument wird in einer ersten Phase in Form von Richtlinien veröffentlicht. Eine Kontrolle der Konformität mit diesen Richtlinien wird vom BAKOM nicht vorgenommen, die Umsetzung der Richtlinien aber dringend empfohlen.

Zu einem späteren Zeitpunkt könnten nötigenfalls die in diesem Dokument enthaltenen Empfehlungen in verbindliche technische und administrative Vorschriften überführt werden.

1.3 Referenzen

[1] SR 784.10
Fernmeldegesetz vom 30. April 1997 (FMG)

[2] ISO/IEC 27001:2005
Information technology – Security Techniques – Information Security Management Systems - Requirements

[3] ISO/IEC 27002:2005
Information technology – Code of Practice for Information Security Management

[4] ISO/IEC 27011:2008
Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

[5] ITU-T X.1051 (02/08)
Information Security Management – Guidelines for Telecommunications based on ISO/IEC 27002

[6] ETSI White Paper No 1, Second Edition, October 2008
Security for ICT – The work of ETSI

Die Empfehlungen der ITU-T können bei der Internationalen Fernmeldeunion, Place des Nations, 1211 Genève 20 (www.itu.int) bezogen werden.

Die ISO-Normen sind beim Zentralsekretariat der Internationalen Organisation für Normung (ISO), 1, rue de Varembé, 1211 Genève (www.iso.ch) erhältlich.

Die Dokumente des ETSI können beim ETSI, Institut européen des normes de télécommunication, 650 Rue des Lucioles, 06921 Sophia Antipolis, Frankreich (www.etsi.org) bezogen werden.

Die Gesetzestexte mit SR-Angabe sind in der systematischen Sammlung der Bundesgesetze auf der Website www.bk.admin.ch veröffentlicht und können beim BBL, CH-3003 Bern bezogen werden.

1.4 Abkürzungen

BAKOM	Bundesamt für Kommunikation
ETSI	*European Telecommunications Standards Institute* – Europäisches Institut für Telekommunikationsnormen
FDA	Fernmeldedienstanbieterin
FMG	Fernmeldegesetz
ICT	*Information and communication technology* – Informations- und Kommunikationstechnologie
ISMS	*Information Security Management System*
ISO	*International Organization for Standardization* – Internationale Organisation für Normung
ITU-T	*International Telecommunication Union, Telecommunication Standardization Sector* - Internationale Fernmeldeunion, Sektor für Telekommunikationsstandardisierung
NIST	*National Institute of Standards and Technology* - Nationales Institut für Normen und Technologie (USA)

1.5 Definitionen

Fernmeldedienst: Fernmeldetechnische Übertragung von Informationen für Dritte.

Information Security Management System: Teil des globalen Management-Systems, dessen Gegenstand die Herstellung, Umsetzung, Nutzung, Überwachung, Überarbeitung, Erhaltung und Verbesserung der Informationssicherheit auf der Grundlage der Risiken ist.

Kontinuitätsplan (Business Continuity Plan): Dokument, das die technischen, vertraglichen, organisatorischen und menschlichen Mittel für die Reaktion eines Unternehmens auf eine Krise festhält.

Sicherheitspolitik: Referenzdokument, in dem die Sicherheitsziele, welche für die Einrichtungen einer Organisation erreicht werden müssen, definiert sind.

Verfügbarkeit: Bereitstellen der Informationen und der daran gebundenen Güter an den berechtigten Benutzer, wenn es nötig ist.

Wiederherstellungsplan (Disaster Recovery Plan): Dokument, das alle detaillierten Verfahren zur Wiederherstellung jeder kritischen Umgebung des Informationssystems nennt.

2 Richtlinien

1) Jede FDA[1] sollte ein Information Security Management System (ISMS) ausarbeiten, dokumentieren, umsetzen, nutzen, überwachen, überarbeiten und laufend verbessern, wie es in der Norm ISO/IEC 27001:2005 [2] beschrieben ist. Für die Wahl der im Rahmen des ISMS (vgl. Anhang 1) vorgesehenen Kontrollen sollte sie sich zudem auf die Empfehlung ITU-T X.1051 [5], die Norm ISO/IEC 27002:2005 [3] oder die Norm ISO/IEC 27011:2008 [4] stützen.

2) Jede FDA sollte einen Kontinuitätsplan (Business Continuity Plan) und einen Wiederherstellungsplan (Disaster Recovery Plan) ausarbeiten, dokumentieren, umsetzen, überarbeiten und laufend verbessern, die namentlich auf ihrer Sicherheitspolitik und auf ihrem ISMS basieren.

3) Jede FDA sollte sich vergewissern, dass ihre Verfahren und ihre Infrastruktur den anerkannten Normen im Bereich der Sicherheit von Informationen und Fernmeldeinfrastrukturen entsprechen (vgl. Anhang 2).

Biel, den 8. Mai 2009

BUNDESAMT FÜR KOMMUNIKATION

Der Direktor:

Martin Dumermuth

[1] Die Liste der FDA, die allesamt von diesen Richtlinien betroffen sind, ist auf der BAKOM-Website unter http://www.bakom.admin.ch/themen/telekom/00462/00794/index.html?lang=de verfügbar.

Anhang 1

Das Information Security Management System (ISMS)

Für Unternehmen, die Dienste im Bereich der Informations- und Telekommunikations-gesellschaft anbieten, sind die Infrastruktur und die darin erzeugten und verwalteten Informationen wichtige Güter. Ein gewissenhaftes Management der Sicherheit dieser Güter ist unerlässlich, damit diese Unternehmen die Zuverlässigkeit ihrer Geschäftstätigkeit gewährleisten und dadurch das Vertrauen ihrer Geschäftspartner gewinnen können.

Im Hinblick auf dieses Ziel beschreibt die Norm ISO/IEC 27001:2005 [2] eine Methode, welche die Ausarbeitung, Umsetzung, Beherrschung und ständige Verbesserung eines Information Security Management Systems (ISMS) ermöglicht. Dieses Dokument richtet sich an die Unternehmensleitungen und an die Mitarbeitenden, die für das Sicherheitsmanagement verantwortlich sind.

Die Ausarbeitung eines ISMS wird von den Zielen, Bedürfnissen, Anforderungen und Risiken im Zusammenhang mit der Tätigkeit der betreffenden Organisation beeinflusst. Es hängt im Übrigen von den eingesetzten Technologien, der Kundschaft sowie der Grösse und Struktur des Unternehmens ab. Jegliche Veränderung dieser Kriterien muss eine Anpassung des Security Management Systems auslösen.

Die Norm ISO/IEC 27001:2005 [2] wird sowohl von den eigenen Mitarbeitenden einer Organisation als auch von beauftragten externen Evaluationsstellen verwendet. So kann eine unabhängige Evaluation durch eine akkreditierte Zertifizierungsstelle zu einer anerkannten Zertifizierung führen, die belegt, dass das betreffende Unternehmen das Sicherheitsmanagement beherrscht.

Das in diesem Dokument vorgeschlagene Modell befolgt den Grundsatz der ständigen Verbesserung durch die vier Phasen «*PLAN-DO-CHECK-ACT*» (PDCA), die regelmässig wiederholt werden. Dieses Modell wird auch im Rahmen anderer Management-Systeme umgesetzt, wie der Norm ISO 9001, deren Ziel das Qualitätsmanagement ist. Es hat den Vorteil, dass es auf alle ISMS angewandt werden kann, unabhängig von der Grösse und Tätigkeit einer Organisation.

Ziel der Planungsphase des Modells (*PLAN*) ist, den Rahmen des Security Management Systems zu definieren. Sie erfordert die Identifizierung und Evaluation der Risiken, die das Unternehmen eingeht. Weiter ist eine Sicherheitspolitik zu definieren, welche die Ziele der Unternehmensleitung beschreibt und die Risiken berücksichtigt, die einen Einfluss auf die Festlegung der Sicherheitszone haben. Orientiert sich die Organisation an den Dokumenten ISO/IEC 27002:2005 [3], ISO/IEC 27011:2008 [4] oder ITU-T X.1051 [5] ist sie im Übrigen dazu gehalten, Kontrollen zu wählen, die der definierten Politik und den Risiken entsprechen, vor denen sich zu schützen sie sich entschieden hat. Die von der ISO mit der Referenz ISO/IEC 27011:2008 [4] herausgegebene Empfehlung ITU-T X.1051 [5] lehnt sich stark an die Norm ISO/IEC 27002:2005 [3] an und findet vor allem im Fernmeldebereich Anwendung. Die getroffene Auswahl der Kontrollen muss danach in einem Dokument mit dem Titel «Statement of applicability» angegeben werden. Es ist letztlich Sache der Unternehmensleitung, den Verfahren, Kontrollzielen und ausser Acht gelassenen Restrisiken zuzustimmen.

Die zweite Phase (*DO*) zielt auf die Umsetzung und Nutzung der geplanten Verfahren und Kontrollen ab.

In der nachfolgenden Phase *(CHECK*) ist die Überwachung und Bewertung der umgesetzten Verfahren und Kontrollen vorgesehen, unter Berücksichtigung der Sicherheitspolitik, der Ziele der Organisation und der praktischen Erfahrung. Diese Analyse muss auch der

Entwicklung der Technologien, der Organisation und des rechtlichen Umfeldes Rechnung tragen. Auch die Bedeutung der ausser Acht gelassenen Restrisiken ist neu einzuschätzen, und jeglicher Sachverhalt, der festgestellt wurde und die Leistungsfähigkeit und Effizienz des ISMS beeinflussen könnte, ist zu berücksichtigen. Schliesslich ist die Unternehmensleitung gehalten, diese Analyse zu genehmigen.

In der letzten Phase (*ACT*) ist vorgesehen, Korrektur- und Vorbeugungsmassnahmen zu ergreifen, die auf den Ergebnissen der Analyse basieren, die im Verlauf der vorangehenden Phase zur Verbesserung des ISMS vorgenommen wurde. In dieser Phase ist es auch erforderlich, alle Betroffenen zu informieren.

Es ist nötig, regelmässig die vier oben beschriebenen Phasen zu durchlaufen, um die ständige Verbesserung des Security Management Systems und damit seiner Zuverlässigkeit zu erreichen.

Anhang 2

Anerkannte Normen für die Sicherheit der Information und der Telekommunikationsinfrastrukturen

Gemäss den Richtlinien zur Sicherheit und Verfügbarkeit von Fernmeldeinfrastrukturen und -diensten (Kap. 2, Ziff. 3) sollte sich jede FDA vergewissern, dass ihre Verfahren und ihre Infrastruktur den anerkannten Normen im Bereich der Sicherheit von Informationen und Fernmeldeinfrastrukturen entsprechen.

Auf diesem Gebiet haben die Standardisierungsorganisationen viele Dokumente ausgearbeitet. Ihre Umsetzung hängt aber von der eingerichteten Infrastruktur und den angebotenen Diensten ab. Zweck dieses Anhangs ist, die FDA über die Normen zu informieren, die zur Anwendung gelangen könnten:

- Das Europäische Institut für Telekommunikationsnormen (ETSI) hat das Dokument «ETSI White Paper No. 1 – Security for ICT» [6] herausgegeben. Dieses gibt einen Überblick über die Standardisierungsprojekte und die zahlreichen technischen Spezifikationen, die es im Bereich der Sicherheit der Informations- und Kommunikationstechnologien erarbeitet hat.

- Der Standardisierungssektor der Internationalen Fernmeldeunion (ITU-T) hat ausserdem Informationen über seine Arbeiten im Bereich der Sicherheit der Informations- und Kommunikationstechnologien (Security Compendium) herausgegeben. Zudem hat er die «ICT Security Standards Roadmap» erstellt. Diese liefert wertvolle Informationen über die existierenden Unterlagen und die laufenden Arbeiten innerhalb verschiedener Standardisierungsorganisationen.

Die durch die Standardisierungsorganisationen ausgearbeiteten Dokumente sind über die BAKOM-Website

http://www.bakom.admin.ch/themen/telekom/00462/01477/03148/index.html?lang=de verfügbar.