BAKOM
OFCOM
UFCOM
UFCOM

Richtlinien zur Sicherheit und Verfügbarkeit von Fernmeldeinfrastrukturen und -diensten

Ausgabe 1:

Inkrafttreten:

BAKOM Bundesamt für Kommunikation
OFCOM Office fédéral de la communication
UFCOM Ufficio federale delle communicazioni
UFCOM Uffizi federal da communicaziuns

Zukunftstrasse 44 / Rue de l'Avenir 44
Postfach / Case postale
CH-2501 Biel/Bienne
www.bakom.ch / www.ofcom.ch

Inhaltsverzeichnis

1 Allgemeines 3
1.1 Geltungsbereich 3
1.2 Stellenwert dieser Richtlinien 3
1.3 Referenzen 3
1.4 Abkürzungen 4
1.5 Definitionen 4
2 Richtlinien 5

1 Allgemeines

1.1 Geltungsbereich

Das Fernmeldegesetz (FMG) [1] hat u.a. zum Ziel, das der Bevölkerung und Wirtschaft qualitativ hoch stehende Fernmeldedienste angeboten werden und ein störungsfreier Fernmeldeverkehr gewährleistet ist (Art. 1 FMG). Die Telekommunikation basiert definitionsgemäss aus miteinander kommunizierendenTeilnetzen, die einander beeinflussen und von einander 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 Mindestsicherheitssystem das jede Fernmeldedienstanbieterin gewährleisten sollte, um zur Zuverlässigkeit und Verfügbarkeit des gesamten nationalen Fernmeldewesens beizutragen.

Diese Richtlinien haben einen Empfehlungsstatus und gelten für die öffentlichen Fest- und Funknetze, womit in der normalen Lage Sprach- und Datendienste hergestellt werden.

Die Richtlinien können ebenfalls in den Zusammenhang der im Rahmen der Revision des FMG geplanten Bestimmung zur Sicherheit und Verfügbarkeit gestellt werden (Art. 48a E-FMG).

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 Form von Richtlinien veröffentlicht. Eine Bewertung der Konformität mit diesem Dokument wird nicht verlangt, die Umsetzung der Richtlinien aber dringend empfohlen.

1.3 Referenzen

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

[2] SR 784.101.1
Verordnung vom 31. Oktober 2001 über Fernmeldedienste (FDV)

[3] ISO/IEC 17799:2005
Information technology – Code of practice for Information Security Management

[4] ITU-T X.1051 (07/2004)
Information Security Management – Requirements for Telecommunications (ISMS-T)

[5] ITU-T E.408 (05/2004)
Telecommunication Networks Security Requirements

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

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

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

1.4 Abkürzungen

BAKOM	Bundesamt für Kommunikation
FDA	Fernmeldedienstanbieterin
FDV	Fernmeldedienstverordnung
FMG	Fernmeldegesetz
ISMS	Information Security Management System
ISO	International Organization for Standardization – Internationale Organisation für Normung
ITU-T	Internationale Fernmeldeunion, Sektor für Telekommunikationsstandardisierung

1.5 Definitionen

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 Ressourcen einer Organisation erreicht werden müssen, definiert sind.

Verfügbarkeit: Das Bereitstellen von Informationen und daran gebundene Ressourcen und Diensten für berechtigte Nutzer.

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

2 Richtlinien

1) Jede FDA sollte eine Sicherheitspolitik ausarbeiten, dokumentieren, umsetzen, unterhalten und verbessern.

2) Jede FDA sollte ein Information Security Management System (ISMS) gemäss der Empfehlung ITU-T X.1051 [4] ausarbeiten, dokumentieren, umsetzen, nutzen, überwachen, unterhalten und verbessern.

3) Jede FDA sollte sicherstellen, dass die Verfahren und Kontrollen ihres ISMS:

- auf der Liste der Kontrollen in Anhang A zur Empfehlung ITU-T X.1051 [4] und auf den Kontrollen in der Norm ISO/IEC 17799:2005 [3] basieren;
- den Anforderungen der Empfehlung ITU-T E.408 [5] entsprechen;
- ihrer Sicherheitspolitik entsprechen.

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

5) Jede FDA sollte sicherstellen, dass ihre Verfahren und ihre Infrastruktur den anerkannten Standards im Bereich der Informations- und Infrastruktursicherheit entsprechen.

Biel, den

BUNDESAMT FÜR KOMMUNIKATION

Der Direktor: