GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

ITSR·sys

Förderungskennzeichen: 16KI81225K

Modell eines IT-Sicherheitsrechts
Allgemeiner Teil

Abschnitt 1: Regelungszweck, Begriffsbestimmungen und Betreiberpflichten

§ 1 Zweck der Regelung

Zweck der Regelungen ist die Gewährleistung von Sicherheit in der Informationstechnik.

§ 2 Begriffsbestimmungen

Im Sinne dieses Gesetzes bezeichnet,

1. „Informationstechnik“ die technischen Mittel zur automatisierten Verarbeitung von Daten in Form von
   a) Komponenten als abgrenzbare Teilfunktionen eines Systems;
   b) Systemen als abgrenzbare und zusammengehörige Einheiten von Funktionen;
   c) Diensten als das zweckspezifische Leistungsangebot von Systemen;

2. „Systemgrenzen“ sämtliche Systeme, deren Funktionen zur Realisierung der betreffenden Dienste eingesetzt werden und die durch den Betreiber kontrolliert werden;

3. „Verarbeitung“ jeder Vorgang oder jede Vorgangsreihe wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten;

4. „Informationstechnisches Produkt“ ein Marktangebot von Informationstechnik;

5. „Sicherheit in der Informationstechnik“ der in Systemen gewährleistete angemessene Schutz vor Ereignissen welche,
   a) die Verfügbarkeit, Authentizität, Integrität, Vertraulichkeit (Schutzziele) von Informationstechnik und
   b) die Schutzziele hinsichtlich der verarbeiteten Daten, sowie
   c) die Funktionalität eines Dienstes betreffen.

   Dies umfasst auch die Gewähr der Resilienz der Systeme;

6. „angemessener Schutz“ die Anwendung technischer und organisatorischer Maßnahmen unter Berücksichtigung des Standes der Technik, die eine zu ihrem Aufwand verhältnismäßige Risikoreduktion bewirken;

7. „technisch-organisatorische Maßnahmen“ alle Mittel und Verfahren, die zur Gewährleistung der Sicherheit in der Informationstechnik eingesetzt werden können;

8. „Stand der Technik“ jene technisch-organisatorischen Maßnahmen, welche die schutzgutabhängigen Schutzziele fördern, sowie fortgeschritten, allgemein anerkannt und praktisch erprobt sind;

9. „Schutzgüter“ die nach den jeweiligen Fachgesetzen zu schützenden Individual- und Gemeinschaftsrechtsgüter;

10. „Risiko“ ist die Unsicherheit über das Auftreten von Ereignissen mit informationstechnischen Auswirkungen und möglichen Schadfolgen an Schutzgütern. Es wird als Kombination aus der Eintrittswahrscheinlichkeit von Ereignissen und der Höhe der Schadfolgen mit vernünftigem Aufwand auf empirischer Basis berechnet oder fundiert geschätzt.

11. „Risikomanagementsystem“ ein iterativer Prozess von Kontexterstellung, Risikoidentifikation, -analyse -bewertung und -behandlung;

12. „informationstechnische Auswirkung“ jede Beeinträchtigung der Sicherheit in der Informationstechnik;

13. „Ereignis“ jede vorsätzliche oder fahrlässige Handlung sowie jeder Zufall (Einwirkungen), welche eine informationstechnische Auswirkung haben kann;

14. „Resilienz“ die Fähigkeit, trotz unmittelbar bevorstehender oder bereits eingetretener Ereignisse die Sicherheit in der Informationstechnik durch eine Adaption aufrechtzuerhalten oder schnellstmöglich wiederherzustellen;

15. „Betreiber“, Jede natürliche oder juristische Person, die Zwecke eines Dienstes festlegt und soweit sie über die eingesetzten Systeme tatsächlich oder rechtlich verfügt;

§ 3 Gewährleistung von Sicherheit in der Informationstechnik

Betreiber haben auf der Grundlage eines Risikomanagementsystems die Sicherheit in der Informationstechnik zu gewährleisten.

Abschnitt 2: Allgemeine Anforderungen an das Risikomanagementsystem

§ 4 Kontexterstellung

(1) Der Betreiber hat auf Basis der sektoralen Schutzgüter relevante Systeme und Dienste zu bestimmen.

(2) Davon ausgehend hat er die Systemgrenzen zu bestimmen und für das weitere Risikomanagement zu dokumentieren. Es sind auch die über Schnittstellen auf die kontrollierten Systeme einwirkenden Drittdienste zu berücksichtigen.

(3) Dabei sind den Daten und der Informationstechnik auch die Schutzziele zuzuordnen, deren Beeinträchtigung eine Verletzung der Schutzgüter nach sich ziehen können.

§ 5 Risikoidentifikation

(1) Die Betreiber haben mit vernünftigem Aufwand alle extern und intern veranlassten Risiken zu identifizieren.

(2) Die Identifikation bezieht sich dabei insbesondere auf

- Risikoquellen jeder Art und jeden Ursprungs einschließlich Drittdiensten,

- mögliche künftige und vergangene Ereignisse, mit informationstechnischen Auswirkungen, die von diesen Risikoquellen ausgehen können,
- Schwachstellen technischer, organisatorischer oder menschlicher Art,
- vorhandene Maßnahmen und
- mögliche kausale Schadfolgen an den relevanten Schutzgütern.

(3) Dies schließt die Nutzung von Warn- und Informationsdiensten nach § 10 sowie die aktive und regelmäßige Durchführung von Testverfahren zur Aufdeckung von Schwachstellen mit ein.

§ 6 Risikoanalyse

(1) Die Risiken sind jeweils in ihrer Höhe zu bemessen. Zur Bemessung der Ereigniswahrscheinlichkeit und der möglichen Schadfolgen kann eine empirisch fundierte quantitative, eine subjektiv schätzende qualitative oder eine kombinierende semi-quantitative Bewertung der Ereigniswahrscheinlichkeit und der möglichen Schadfolgen gewählt werden.

(2) Die Berechnung der Wahrscheinlichkeit von Ereignissen soll auf Basis empirischer Daten vorgenommen werden, sofern diese Daten bereits erhoben sind oder mit vernünftigem Aufwand erhoben werden können. Andernfalls sind fundierte Schätzungen vorzunehmen.

(4) Schließlich sind das Gewicht der informationstechnischen Auswirkungen der Ereignisse sowie die daraus resultierende- Höhe der Schadfolgen für Schutzgüter zu analysieren.

(5) Handelt es sich bei der identifizierten Risikoquelle um eine natürliche Person, sind insbesondere auch deren Motivation, Fähigkeiten, und Ressourcen abzuschätzen.

(6) Soweit Risiken nicht identifiziert oder vollständig analysiert werden können (Ungewissheit), aber für kritisch betroffene Schutzgüter vermutet werden, ist dies als Ausgangspunkt für Maßnahmen nach § 10 zu dokumentieren.

§ 7 Risikobewertung

(1) Im Rahmen der Risikobewertung sind die jeweils identifizierten und bemessenen Risiken für die Schutzgüter mit dem Aufwand für mögliche Maßnahmen ins Verhältnis zu setzen.

(2) Bei der Maßnahmenwahl ist der Stand der Technik zu berücksichtigen. Der Stand der Technik ist mit Blick auf die Risiken objektiv zu bestimmen. Vorhandene Veröffentlichungen oder Feststellungen zuständiger Behörden können als Stand der Technik angenommen werden, wenn die Anwendbarkeit für die analysierten Risiken gewährleistet ist.

(3) Die Maßnahmen sind dabei mit Blick auf ihre risikoreduzierende Wirkung, insbesondere auf die Wahrscheinlichkeit des Auftretens einer informationstechnischen Auswirkung zu untersuchen. Anschließend ist zu untersuchen, ob das Risiko sich hierdurch soweit reduzieren lässt, dass ein angemessener Schutz erreicht wird. Ist dies nicht der Fall, sind weitere oder wirksamere Maßnahmen zu betrachten.

(4) Das Erfordernis an Maßnahmen kann im Einzelfall über den Stand der Technik hinausgehen oder innerhalb der Grenzen des Abs. 2 Satz 1 hinter diesem zurückbleiben. Letzteres ist in der Dokumentation gemäß § 11 besonders zu begründen.

§ 8 Risikobehandlung

(1) Die Maßnahmen sind unverzüglich umzusetzen. Nach Vornahme aller Maßnahmen sind diese auf ihre beabsichtigte Gesamtwirksamkeit hin zu überprüfen.

(2) Ist durch die Maßnahmen kein angemessener Schutz im Sinne des § 7 Abs. 3 erreichbar, ist der Einsatz der Informationstechnik in seiner konkreten Gestalt unzulässig.

§ 9 Iteration

Der Risikomanagementprozess ist turnusmäßig zu wiederholen. Der Turnus bestimmt sich insoweit nach der Bedeutung der gefährdeten Schutzgüter. Ungeachtet dessen ist der Risikomanagementprozess bei wesentlichen Veränderungen der sicherheitskritischen Sach- oder Informationslage (z.B. in der Informationstechnik) unverzüglich zu wiederholen.

§ 10 Beobachtungspflichten

Betreiber haben sich mittels öffentlich zugänglicher Warn- und Informationsdienste fortwährend über Schwachstellen zu informieren. Das Auftreten und das Behandeln einer Schwachstelle gilt als wesentliche Veränderung i.S.d. § 9 S. 3.

§ 11 Maßnahmen zur Resilienz

(1) Maßnahmen zur Resilienz sind so auszugestalten, dass der im Rahmen des Risikomanagements verbleibenden Ungewissheit (§ 6 Abs. 4) bestmöglich begegnet wird.

(2) Weiterhin sind Resilienzmaßnahmen auch hinsichtlich der Ungewissheit zu ergreifen, die aus der Verwendung von Drittdiensten resultiert.

(3) § 9 gilt entsprechend.

§ 12 Dokumentation

Die Durchführung des Risikomanagements ist zu dokumentieren. Im Rahmen der Risikobewertung schließt dies die Begründung für die Wahl der jeweiligen Maßnahmen mit ein.

Abschnitt 3: Fachgesetzliche Anforderungen

§ 13 Normative Gestaltungsziele

Die Anforderungen an die Sicherheit in der Informationstechnik können durch Fachgesetze über die genannten Schutzziele hinaus um besondere Ausprägungen erweitert werden, die den jeweiligen Anforderungen Rechnung tragen.

§ 14 Konkretisierung von Beobachtungspflichten

Die Anforderungen an die Beobachtungspflichten können durch Fachgesetze konkretisiert werden. Dies umfasst insbesondere die Benennung einzelner Warn- und Informationsdienste privater und öffentlicher Stellen (z.B. CERT-Bund), welche von spezifischen Gruppen von Betreibern und methodisch im Rahmen der Risikoidentifikation zwingend zu nutzen sind.

§ 15 Konkretisierung des Stands der Technik

Die Anforderungen an die Einbeziehung des Stands der Technik können fachgesetzlich konkretisiert werden. Auch kann der Stand der Technik durch die Fachgesetze inhaltlich näher konturiert werden. Schließlich kann in Fachgesetzen statt des Standes der Technik auch auf die anerkannten Regeln der Technik oder den Stand der Wissenschaft und Technik verwiesen werden.

Abschnitt 4: Verwaltungsrechtliche Vorgaben

§ 16 Meldungen

(1) Meldungen über informationstechnische Auswirkungen erfolgen im fachgesetzlich definierten Umfang an die zuständige Aufsichtsbehörde.

(2) Die Aufsichtsbehörde nutzt diese Meldungen, um über empirisch ermittelte Entwicklungen in der IT-Sicherheitslage zu informieren, Schwachstellendatenbanken zur Verfügung zu stellen sowie um vor entdeckten Schwachstellen zu warnen.

(3) Sowohl die Meldungen der als auch die Warnungen an die Betreiber erfolgen in einem von der Aufsichtsbehörde zu definierenden, einheitlichen elektronischen Datenformat.