

IT-Sicherheit

Grundsätze zur IT-Sicherheitspolitik des BM.I

Versionen:

Die angeführten Versionen sind vom IT-Sicherheitsbeauftragten des BM.I zur Veröffentlichung freigegeben.

Version 1.0 1. September 2003

Version 1.0.1 August 2004 Anpassung an das Corporate Design des BM.I

1 PRÄAMBEL	1
2 EINORDNUNG DES DOKUMENTS	3
3 ALLGEMEINE FESTLEGUNGEN	5
3.1 AUFGABEN UND ZIELE DER IT-SICHERHEITSPOLITIK	5
3.2 BEGRIFFSBESTIMMUNGEN.....	5
3.2.1 Informationen	5
3.2.2 Informationssysteme	6
3.2.3 Informationssicherheit.....	6
3.2.4 IT-Sicherheit.....	6
3.3 GELTUNGSBEREICH.....	6
3.4 PUBLIKATION DER IT-SICHERHEITSPOLITIK.....	7
4 GRUNDSÄTZLICHE ZIELE UND STRATEGIEN	9
4.1 SICHERHEITZIELE	9
4.2 SICHERHEITSNIVEAU.....	9
4.3 STRATEGIEN FÜR DAS IT-SICHERHEITSMANAGEMENT	10
5 VERANTWORTLICHKEITEN UND PFLICHTEN	12
5.1 LEITUNG DES RESSORTS	12
5.2 FÜHRUNGSKRÄFTE.....	13
5.3 STEUERUNGSGREMIUM FÜR INFORMATIONSTECHNOLOGIE (SIT)	14
5.4 IT-SICHERHEITSORGANISATIONSSTRUKTUR	15
5.4.1 IT-Sicherheitsbeauftragter des Ressorts.....	15
5.4.2 IT-Sicherheitsmanagement-Team (IST).....	15
5.4.3 IST-Büro	17
5.4.4 Bereichs IT-Sicherheitsbeauftragte	18
5.4.5 System IT-Sicherheitsbeauftragte	19
5.4.6 IT-Sicherheitsvertrauenspersonen (ISV).....	20
5.5 APPLIKATIONS- UND PROJEKTVERANTWORTLICHE.....	20
5.6 MITARBEITER	21
6 RISIKOSTRATEGIEN, RESTRISIKO UND RISIKOAKZEPTANZ	22
7 MAßNAHMEN ZUR IT-SICHERHEIT	24
7.1 KLASSIFIZIERUNG VON INFORMATIONEN UND IT-ANWENDUNGEN.....	24
7.2 INTEGRITÄT VON DATEN UND INFORMATIONSSYSTEMEN	26
7.3 ORGANISATIONSWEITE RICHTLINIEN ZU SICHERHEITSMABNAHMEN.....	27
7.4 DISASTER RECOVERY PLANUNG.....	28
7.5 NACHFOLGEAKTIVITÄTEN ZUR ÜBERPRÜFUNG UND AUFRECHTERHALTUNG DER IT-SICHERHEIT	28
7.6 IT-SICHERHEITSDOKUMENTATION DES BML.....	29
8 LIFE CYCLE DER IT-SICHERHEITSPOLITIK	30

1 Präambel

Das Bundesministerium für Inneres (BMI) hat den Auftrag, die Innere Sicherheit dieses Landes zu gewährleisten und zukunftsweisend auszubauen. Es repräsentiert dabei in Österreich das größte und sensibelste Dienstleistungsunternehmen im Bereich Sicherheit, dessen erfolgreiche Arbeit dabei immer mehr vom Einsatz moderner Informationstechnologie (IT) bestimmt wird. Der ungestörte Ablauf der Geschäftsprozesse und das Image des Ressorts ist daher in den Augen der Öffentlichkeit zu einem großen Teil abhängig von der Vertraulichkeit, Integrität und Verfügbarkeit der Kommunikation, Speicherung und Verarbeitung der zur Aufrechterhaltung der öffentlichen Sicherheit und Ordnung benötigten Informationen.

Diese Informationen sind als immaterielles Betriebsvermögen zu betrachten und die für deren Verarbeitung und Kommunikation benutzten Komponenten sind wertvolle und schützenswerte Ausstattung des Ressorts. Zielsetzung ist es, den Verlust, die Verfälschung beziehungsweise Manipulation und die unerwünschte Offenlegung aller für den geordneten Geschäftsbetrieb wichtigen Informationen zu verhindern.

Alle Mitarbeiter sind daher persönlich verpflichtet, ressortinterne Informationen und die damit verbundene Infrastruktur gegen Verlust und Missbrauch jeglicher Art zu schützen.

Das Thema Informationssicherheit (IS) hat in den letzten Jahren in zunehmendem Maße internationale Organisationen beschäftigt, woraus im Rahmen der EU-Mitgliedschaft auch rechtsverbindliche Bedeutung für die Hoheitsverwaltung resultiert. Die Europäische Kommission hat in ihrer Mitteilung *Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz* (Juni 2001) die Wichtigkeit dieser Problematik hervorgehoben: „Sicherheit ist auf dem Weg, eine Priorität zu werden, weil Kommunikations- und Informationsinfrastrukturen ein wichtiger Faktor für wirtschaftliche und soziale Entwicklung geworden sind. Netze und Informationssysteme ermöglichen Dienstleistungen und übertragen Daten in einem Maße, in dem dies noch vor wenigen Jahren unvorstellbar war. Ihre Verfügbarkeit ist für andere Infrastrukturen wie etwa Wasser- oder Stromversorgung unerlässlich. Je mehr jedermann, ob Unternehmen, Bürger oder öffentliche Verwaltungen, die Möglichkeiten der Kommunikationsnetze nutzen möchte, desto mehr wird die Sicherheit dieser Systeme zu einer Voraussetzung für weiteren Fortschritt.“

Die Kommission empfiehlt den Mitgliedstaaten, beispielhafte Maßnahmen wie z.B. die einschlägigen ISO-Standards zu fördern. Der Rat der Europäischen Union hat diese Empfehlung in einer *Entschließung zu einem gemeinsamen Ansatz und spezifischen Maßnahmen im Bereich der Netz- und Informationssicherheit* (Dezember 2001) bekräftigt.

In diesem Zusammenhang sieht das österreichische Strafrechtsänderungsgesetz 2002 u.a. die Schaffung von neuen Deliktstatbeständen, auch in Umsetzung der Cybercrime-Konvention des Europarates vom November 2001, z.B. bzgl. „Widerrechtlicher Zugriff auf ein Computersystem“, „Störung der Funktionsfähigkeit eines Computersystems“, „Missbräuchliches Abfangen von Daten“ oder „Datenfälschung ,vor“.

2 Einordnung des Dokuments

IT-Sicherheitsmanagement ist ein kontinuierlicher Prozess, der die Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Verbindlichkeit und Zuverlässigkeit von Systemen und Verfahren der Informationstechnik gewährleisten soll. Die Strategien und Konzepte dieses Prozesses sind laufend auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf in angemessener Form fortzuschreiben und anzupassen.

Folgende Darstellung (Abb. 1) zeigt den Aufbau des IT-Sicherheitsmanagementprozesses. Mit diesem Dokument wird in einem ersten Schritt die Entwicklung einer organisationsweiten IT-Sicherheitspolitik abgedeckt. Die weiteren Prozessschritte sind im österreichischen IT-Sicherheitshandbuch (ITSHB) im Detail beschrieben.

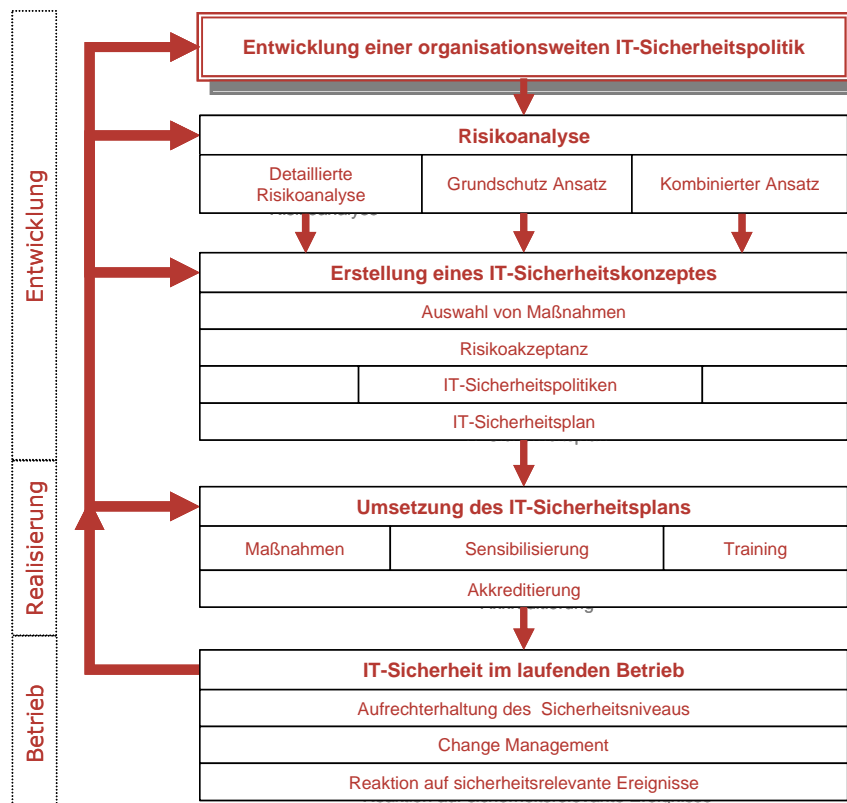


Abb. 1

Die Vorgehensweise nach dem österreichischen IT-Sicherheitshandbuch wurde naheliegenderweise deshalb gewählt, weil einerseits das Bundesministerium für Inneres die treibende Kraft bei der Erstellung des Handbuches darstellte und somit direkt auf einen Teil der Know-How-Träger zugegriffen werden kann und andererseits bietet das österreichische IT-Sicherheitshandbuch auf die österreichischen Rechtsnormen, Standards und Terminologien angepasste Leitlinien und Vor-

gaben, die praktisch alle wesentlichen für die Informationssicherheit relevanten internationalen Standards (z.B. ISO TR 13335, BS 7799 bzw. ISO 17799, ITSEC, ISO 15408/ Common Criteria) und Leitlinien (z.B. BSI Sicherheitshandbuch, BSI Grundschutzhandbuch) einschließen.

3 Allgemeine Festlegungen

Hinweis: Sämtliche in diesem Dokument verwendeten Funktionsbezeichnungen sind geschlechtsneutral zu verstehen.

3.1 Aufgaben und Ziele der IT-Sicherheitspolitik

Die vorliegenden Grundsätze zur IT-Sicherheitspolitik erläutern die Bedeutung von Informationen für das Ressort und bilden den Rahmen für Richtlinien und Maßnahmen im Zusammenhang mit einem sicheren Umgang mit Informationen. Insbesondere sollen sie

- ✍ Verantwortungen regeln,
- ✍ das Bewusstsein für die Notwendigkeiten und Einhaltung aller der Informationssicherheit dienenden Vorkehrungen fördern, insbesondere auch durch die Zusage seitens der Leitung des Ressorts, alle Maßnahmen die die Wichtigkeit des Themas verdeutlichen sollen, zu unterstützen,
- ✍ ein Mindestmaß von Aufgaben und Pflichten festlegen, deren Erfüllung für die Gewährleistung und Aufrechterhaltung einer angemessenen Informationssicherheit unabdingbar sind und
- ✍ die Klassifizierung von Informationen und IT-Anwendungen in Bezug auf Vertraulichkeit, Datenschutz, Integrität und Verfügbarkeit regeln.

3.2 Begriffsbestimmungen

3.2.1 Informationen

Unter Informationen im Sinne der Grundsätze der IT-Sicherheitspolitik sind zu verstehen:

- ✍ Sprachliche Formulierungen,
- ✍ Dokumente und Unterlagen aller Art, die auf Papier oder anderen von Menschen lesbaren Medien vorliegen,
- ✍ Daten (z. B. Texte, Programme, Sprache, Bilder, Videos), die in elektronischer bzw. maschinenlesbarer Form auf Informationsverarbeitungssystemen (z. B. Großrechner, Server, Arbeitsplatzsysteme, Personal Computer, Organizer, Chipkarten o.ä.) verarbeitet oder gespeichert werden,
- ✍ Daten, die auf magnetischen, optischen oder sonstigen maschinenlesbaren Datenträgern gespeichert sind,

- ✗ Informationen, die mit Hilfe von Kommunikationssystemen, -diensten (z. B. Telefon, Mobilfunk, Fax, e-Mail, Funk-LAN, Infrarotschnittstelle etc.) über lokale, ressortweite oder öffentliche Netze übertragen werden.

3.2.2 Informationssysteme

Unter Informationssystemen sollen im Folgenden sowohl Informationsverarbeitungssysteme (inkl. Peripherie) als auch Kommunikationssysteme, -dienste und -netze verstanden werden.

3.2.3 Informationssicherheit

Unter Informationssicherheit wird der Sammelbegriff aller Aspekte zum Schutz von Informationen vor Verlust, unbefugter Veränderung und unbefugter Kenntnisnahme verstanden.

3.2.4 IT-Sicherheit

IT-Sicherheit umfasst alle Aspekte in Verbindung mit der Definition, Erreichung und Aufrechterhaltung von Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit, Authentizität und Zuverlässigkeit in Informationssystemen.

Das Dokument behandelt zwar primär die Aspekte der IT-Sicherheit, es werden jedoch alle relevanten Aspekte der Informationssicherheit mit berücksichtigt, da in praktisch allen Belangen der Informationssicherheit auch Informationssysteme involviert sind.

3.3 Geltungsbereich

Die Grundsätze zur IT-Sicherheitspolitik gelten für das BMI und alle diesem organisatorisch nachgeordneten Behörden und Dienststellen. Sofern in diesem Dokument das BMI genannt wird, ist immer der gesamte Geltungsbereich angesprochen.

Im Falle besonderer Schutzbedürfnisse ist es Teilbereichen des Ressorts (z.B. Bundeskriminalamt, Bundesamt für Verfassungsschutz und Terrorismusbekämpfung) gestattet, eine eigene, den spezifischen Schutzbedürfnissen entsprechende IT-Sicherheitspolitik in Kraft zu setzen. Diese soll mindestens die hier beschriebenen Grundsätze widerspiegeln und kann zusätzliche strategische Details enthalten, um höheren Sicherheitsanforderungen Rechnung zu tragen. Bereiche mit geringerem Schutzbedarf (z.B. Stand-Alone - Internet-PC) sind, mittels einer eigenen, spezifischen IT-Sicherheitspolitik, ebenfalls dem Gesamtgeltungsbereich hinzuzuzählen.

Alle Mitarbeiter im Geltungsbereich sind unabhängig von der Art und dem Umfang ihrer Mitarbeit auf die Grundsätze der IT-Sicherheitspolitik verpflichtet. Eingeschlossen sind auch Mitarbeiter auf Zeit (z. B. Leiharbeitnehmer, Zivildienstleistende, Feriapraktikanten etc.)

Bei der Zusammenarbeit mit Geschäftspartnern ist darauf zu achten, dass diese Grundsätze und die damit verbundenen Maßnahmen zur IT-Sicherheit ebenfalls angewandt werden. Dies gilt insbesondere auch für ressortfremde Bereiche, welche die IT-Infrastruktur des BMI nutzen.

Weitergehende Vereinbarungen zur IT-Sicherheit im Rahmen von externen Kooperationen oder Projekten haben Vorrang gegenüber diesen Grundsätzen, sofern sie nicht den in diesem Dokument festgelegten Mindeststandard an Informations- bzw. IT-Sicherheit unterschreiten.

Gesetzliche Regelungen und Vorschriften zur IT-Sicherheit (z.B. enthalten im Beamten-dienstrechtsgesetz BDG, Vertragsbedienstetengesetz VBG, Datenschutzgesetz DSG, Datenschutzerlass, Informationssicherheitsgesetz InfoSiG, Informationssicherheitsverordnung InfoSiV, Signaturgesetz SigG, Signaturverordnung SigV, materiegesetzliche Regelungen, u.a.) sind unabhängig von diesen Grundsätzen zu beachten.

Sofern Internationale Vereinbarungen und Abkommen die IT-Sicherheit berühren, so sind diese in geeigneter Weise mit einzubeziehen.

Der Schutz des Lebens und der Unversehrtheit von Personen hat ohne Ausnahme Vorrang vor der IT-Sicherheit. Maßnahmen zur IT-Sicherheit dürfen nicht andere Verordnungen (z.B. Brandschutz und Objektschutz) außer Kraft setzen. Im Konfliktfall müssen alternative Maßnahmen erarbeitet werden, die den unterschiedlichen Regelungen insgesamt Rechnung tragen.

3.4 Publikation der IT-Sicherheitspolitik

Die IT-Sicherheitspolitik ist allen Mitarbeitern zur Kenntnis zu bringen und von diesen zu beachten. Mitarbeiter, deren Aufgaben die IT-Sicherheit direkt berühren bzw. Mitarbeiter in führenden Positionen, müssen im Besitz einer aktuellen Version des vorliegenden Dokumentes sein. Konkret zu benennen sind diesbezüglich:

- ✍ das Kabinett des Bundesministers,
- ✍ die leitenden Stellen aller Sektionen,
- ✍ der Leiter der Abteilung Interne Revision
- ✍ der Leiter der Abteilung Interne Angelegenheiten
- ✍ die leitenden Stellen
 - der Sicherheitsdirektionen
 - der Bundespolizeidirektionen
 - der Landesgendarmeriekommanden

- des Bundeskriminalamts
- des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung
- ✗ die leitenden Stellen des Bundesasylamtes
- ✗ die Mitglieder des Steuerungsgremiums für IT (SIT)
- ✗ die Mitglieder des IT-Sicherheitsmanagement-Teams (IST)
- ✗ die Bereichs-IT-Sicherheitsbeauftragten,
- ✗ die Applikations- / Projektverantwortlichen.

4 Grundsätzliche Ziele und Strategien

Ziel der IT-Sicherheit ist, die rechtzeitige, korrekte und sichere Zurverfügungstellung aller für die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung notwendigen Informationen an den berechtigten Personenkreis mittels geeigneter IT-Systeme. IT-Sicherheit ist eine wichtige Voraussetzung für den effizienten Geschäftsablauf innerhalb des BMI, die eine angemessen hohe Verfügbarkeit der Informationssysteme, aktuelle und zuverlässige Daten und einen reibungslosen Informationsfluss erfordert.

4.1 Sicherheitsziele

Die IT-Sicherheit dient dazu, um

- ✎ sicherzustellen, dass die aus gesetzlichen Vorgaben resultierenden Anforderungen erfüllt werden,
- ✎ zu gewährleisten, dass das Vertrauen der Öffentlichkeit und das Ansehen in das BMI und die öffentliche Verwaltung im Allgemeinen gewahrt bleibt,
- ✎ die Kontinuität aller mit Hilfe von Informationstechnologie unterstützten Arbeitsabläufe und Geschäftsprozesse zu gewährleisten,
- ✎ hohe Verlässlichkeit des Handelns zu gewährleisten, insbesondere in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit von Informationen,
- ✎ sicherzustellen, dass Informationen entsprechend ihrer Bedeutung für das Ressort klassifiziert und zusammen mit den zur Verarbeitung und Kommunikation eingesetzten Informationssystemen angemessen geschützt werden,
- ✎ den Verlust und die Verfälschung von Informationen, Informationssystemen und Datenträgern zu vermeiden, zu erkennen und zu beheben,
- ✎ zu verhindern, dass Informationen und Informationssysteme zufällig, fahrlässig oder vorsätzlich Unberechtigten zugänglich gemacht werden bzw. zu nicht genehmigten Zwecken genutzt werden.

4.2 Sicherheitsniveau

Als angemessener Sicherheitslevel wird ein durch den Grundsatzansatz des *Österreichischen IT-Sicherheitshandbuchs* festgelegtes Sicherheitsniveau angestrebt.

Darüber hinaus soll im Bedarfsfall stärkerer Schutzbedürfnisse – in Teilbereichen oder ressortweit – explizit auch ein höheres Niveau angestrebt werden. Dieser Bedarf ist im Rahmen einer IT-Risi-

koanalyse zu klären und soll die Auswahl angemessener Maßnahmen zur Verminderung der Risiken ermöglichen.

Es wird allgemein angenommen, dass es keine wirtschaftlich angemessenen Sicherheitsmaßnahmen gibt, die im laufenden Betrieb vollkommene Sicherheit bieten. Aufgrund des daraus resultierenden Restrisikos ist es erforderlich, zusätzliche Maßnahmen zur Sicherung der Geschäftskontinuität (z.B. Backupkonzepte und Disaster Recovery Planung) zu entwickeln.

4.3 Strategien für das IT-Sicherheitsmanagement

Die Strategie zur IT-Sicherheit des Ressorts wurde in Abstimmung mit der IKT-Strategie des Bundes, durch Mitarbeiter des Ressorts, zusammen mit Fachleuten aus der Wirtschaft, dem A-SIT und der Abteilung IT-MS, erarbeitet.

Durch konsequente Anwendung folgender IT-Sicherheitsstrategien sollen die Sicherheitsziele und das angestrebte, angemessene Sicherheitsniveau erreicht werden:

- ✗ eine organisationsweite Methodik zur IT-Sicherheit (IT-Sicherheitsmanagementprozess),
- ✗ eine klare Zuordnung aller Verantwortlichkeiten im IT-Sicherheitsmanagementprozess,
- ✗ die Festlegung regelmäßiger Überprüfung des IT-Sicherheitsmanagementprozesses (Change Management),
- ✗ die Förderung des Sicherheitsbewusstseins der Mitarbeiter durch Vermittlung von Wissen und sicherheitsrelevantem Verhalten (Security Awareness),
- ✗ die Festlegung eines „Warnsystems“ für wesentliche Vorfälle und Schwachstellen innerhalb des Ressorts,
- ✗ das Feststellen des aktuellen Handlungsbedarfes durch angemessene regelmäßige Risikoanalysen nach dem kombinierten Ansatz lt. ITSHB,
- ✗ die Erstellung und Weiterentwicklung von Sicherheitsplänen zur Etablierung angemessener IT-Sicherheitsmaßnahmen,
- ✗ die regelmäßige Berichterstattung und Dokumentation über den erreichten Stand an das SIT (vierteljährlich) und an die Leitung des Ressorts (jährlich),
- ✗ die Einführung eines IT-Sicherheitsinformationssystems im Intranet, das als Regelwerk zur IT-Sicherheit und als Informationsbibliothek für alle Mitarbeiter für Themen der IT-Sicherheit dienen soll (Knowledge Management).

- ✍ die Festlegung von Sanktionen, die bei Verstößen von Mitarbeitern gegen Richtlinien der IT-Sicherheit von deren Vorgesetzten angewandt werden.

5 Verantwortlichkeiten und Pflichten

Damit die IT-Sicherheit im BMI erfolgreich gelebt wird, ist die organisationsweite Methodik des IT-Sicherheitsmanagementprozesses zu schaffen. Hierbei handelt es sich um einen Prozess, der ständig der Beobachtung und Verbesserung bedarf, um die aktuellen Schutzbedürfnisse zu erfüllen. Dies kann nur durch das Zusammenwirken von Verantwortlichkeiten und Pflichten auf allen Ebenen der Organisation des Ressorts erreicht werden.

Die Verantwortlichkeiten werden von der Leitung des Ressorts auf das Management der Sektionen, Ämter und bedeutender Dienststellen ausgedehnt. Die Führungskräfte verpflichten die Mitarbeiter dazu, die IT-Sicherheitspolitik zu beachten.

Zur Unterstützung der Führungskräfte wird eine IT-Sicherheitsorganisationsstruktur aufgebaut, die den IT-Sicherheitsmanagementprozess verantwortet und Qualitätsmoderation im Management und bei den Mitarbeitern betreibt und kurze Meldewege für sicherheitsrelevante Ereignisse eröffnet. Hierzu zählen der IT-Sicherheitsbeauftragte des Ressorts, das IT-Sicherheitsmanagement-Team, die Bereichs-IT-Sicherheitsbeauftragten, die System-IT-Sicherheitsbeauftragten und die IT-Sicherheitsvertrauenspersonen.

Das Steuerungsgremium für IT-Belange (SIT) und die nachgeordneten Business IT Units (BIT's) arbeiten eng mit der IT-Sicherheitsorganisation zusammen, um die Umsetzung von IT-Sicherheitsmaßnahmen technischer Art zu unterstützen. Neue Maßnahmen werden vom IT-Sicherheitsmanagement-Team priorisiert und im Einvernehmen mit dem SIT in den IT-Gesamtplan aufgenommen.

Das grundsätzliche Ziel der Festlegung einer IT-Sicherheitsorganisationsstruktur ist nicht das Schaffen einer Parallelstruktur zur bestehenden Aufbauorganisation bzw. der IT-Organisationsstruktur des Bundesministeriums für Inneres, sondern eine klare und eindeutige explizite Regelung und Festschreibung bereits bestehender, aber oftmals nur implizit definierter Verantwortlichkeiten und Verpflichtungen, aus dem Blickwinkel eines einheitlichen, organisationsweiten IT-Sicherheitsmanagementkonzepts.

Nachfolgend sind die Rollen im Einzelnen beschrieben:

5.1 Leitung des Ressorts

IT-Sicherheit ist eine Führungsaufgabe, die das gesamte Ressort betrifft. Es liegt daher im Interesse der Ressortleitung,

- ✗ dass die Verantwortung für die in der IT-Sicherheitspolitik formulierten Ziele und Grundsätze übernommen und organisationsweit verankert wird,
- ✗ ausreichend Ressourcen für die Etablierung eines tragfähigen IT-Sicherheitsmanagements genehmigt und zur Verfügung gestellt werden,
- ✗ die Verantwortung für das Restrisiko der operativen Sicherheitsmaßnahmen und der Disaster Recovery-Strategie übernommen wird.

Jede grundsätzliche Änderung der vorliegenden IT-Sicherheitspolitik bedarf zukünftig der Zustimmung der Ressortleitung.

5.2 Führungskräfte

Jede Führungskraft trägt die Verantwortung für die Einhaltung der gültigen IT-Sicherheitsrichtlinien in der Form, dass sie

- ✗ in ihrem Verantwortungsbereich durch das IT-Sicherheitsmanagement-Team veranlasste Untersuchungen auf Schwachstellen der IT-Sicherheit unterstützt,
- ✗ Maßnahmen unterstützt, die bei der Behebung von Schwachstellen und Untersuchung von IT-Sicherheitsvorfällen helfen,
- ✗ nicht behebbare Schwachstellen oder wesentliche Vorfälle innerhalb ihres Verantwortungsbereiches, im Wege des zuständigen Bereichs-IT-Sicherheitsbeauftragten an den IT-Sicherheitsbeauftragten des Ressorts meldet,
- ✗ den Bereichs-IT-Sicherheitsbeauftragten und die IT-Sicherheitsvertrauenspersonen dabei unterstützt, Bewusstseinsbildung zu betreiben und die Mitarbeiter auf die IT-Sicherheitspolitik zu verpflichten,
- ✗ das Informationsbedürfnis der Mitarbeiter im Bezug auf IT-Sicherheit im Rahmen ihrer Möglichkeit fördert und insbesondere den Zugang zu erforderlichen Schulungsmaßnahmen veranlasst,
- ✗ dafür Sorge trägt, dass für wichtige und sensible Informationen der Grad der Vertraulichkeit und Sensibilität entsprechend den Vorgaben der IT-Sicherheitspolitik festlegt wird,
- ✗ die Einhaltung der IT-Sicherheitsrichtlinien und die Wahrung der Sorgfaltspflicht beim Umgang mit Informationen im Rahmen der Dienstaufsicht kontrolliert,
- ✗ im Fall von Verstößen gegen IT-Sicherheitsrichtlinien im Rahmen ihrer Dienstaufsicht die erforderlichen Maßnahmen veranlasst.

5.3 Steuerungsgremium für Informationstechnologie (SIT)

Als zentrales und ressortweit zuständiges Steuerungsgremium für IT arbeitet das SIT die Strategien im IT-Bereich aus. Im Rahmen seiner Tätigkeit entscheidet es über die Durchführung der, im Regelfall aus den BIT's der Sektionen (Business Units für IT) kommenden Projektanträge. Dabei obliegt es dem SIT, eine Reihung der Projekte nach Priorität vorzunehmen. In diesem Zusammenhang entscheidet das SIT auch über die Budgetmittelverwendung und die Projektverantwortung.

In allen Belangen der IT-Sicherheit erfolgt die Ausarbeitung der IT-Sicherheitspolitik, Risikoanalysen, IT-Sicherheitskonzepte (Maßnahmenauswahl, Risikoakzeptanz, IT-Sicherheitspläne), Sensibilisierungs- und Trainingsmaßnahmen sowie der daraus resultierenden Projektanträge durch das IT-Sicherheitsmanagementteam (IST).

Die solcherart ausgearbeiteten Pläne bzw. Projektanträge werden dem SIT durch den IT-Sicherheitsbeauftragten zur Bewertung der Restrisikoakzeptanz und daraus resultierend zur Beauftragung notwendiger, zu implementierenden Maßnahmen, vorgelegt. Durch diese Vorgehensweise ist sichergestellt, dass IT-Sicherheitsprojekte nicht gegen andere IT-Projekte budgetär aufgerechnet, sondern immer nur im Hinblick auf eine eventuell notwendige Sicherheitsrisikominimierung begutachtet werden.

Das SIT ist für die Umsetzung (Realisierung und Beauftragung der Implementierung sowie Initiierung des Betriebs) von IT-Sicherheitsmaßnahmen und daraus resultierend für die Gewährleistung der IT-Sicherheit im laufenden Betrieb verantwortlich. Im Wesentlichen umfasst dies

- ✍ die Umsetzung von Vorschlägen zu IT-Sicherheitsmaßnahmen, die vom IT-Sicherheitsmanagement- Team eingebracht werden,
- ✍ zusammen mit der Leitung des Ressorts die Akzeptanz des Restrisikos von Sicherheitslücken und Schwachstellen, deren weitere Behandlung aus wirtschaftlichen Gründen nicht möglich ist,
- ✍ die Unterstützung der IT-Sicherheitsorganisation und der IT-Betreiber durch die Bereitstellung der notwendigen Mittel für die Aufarbeitung von ressortweiten Vorfällen, welche die IT-Sicherheit betreffen,
- ✍ die umgehende Information des IT-Sicherheitsbeauftragten über IT-sicherheitsrelevante Themen bzw. Projektanträge,
- ✍ die Beauftragung von IT-sicherheitsrelevanten Projekten.

5.4 IT-Sicherheitsorganisationsstruktur

Die IT-Sicherheitsorganisation muss alle Belange der IT-Sicherheit im Ressort operativ abdecken können, dabei ist einerseits auf die starke Dezentralisierung der Dienststellen und andererseits auf die unterschiedlichen Sicherheitsanforderungen in einzelnen Organisationsbereichen Rücksicht zu nehmen.

Die Organisationsstruktur der für die IT-Sicherheit zuständigen Funktionen und Personen wird allen Mitarbeitern des BMI in geeigneter Weise in der jeweils gültigen Form zur Kenntnis gebracht.

5.4.1 IT-Sicherheitsbeauftragter des Ressorts

Der IT-Sicherheitsbeauftragte des BMI wird von der Leitung des Ressorts bestellt und kommt aus dem laut der Geschäftseinteilung des BMI für die IT-Sicherheit zuständigen Organisationsbereich. Er trägt die Gesamtverantwortung für das Qualitätsmanagement der IT-Sicherheit im Ressort.

Zu seinen Pflichten gehört

- ✗ die verantwortliche Mitwirkung an der Erstellung des IT-Sicherheitskonzeptes,
- ✗ die Aufrechterhaltung eines entsprechend qualitativen IT-Sicherheitsmanagementprozesses,
- ✗ Auswahl und Planung der ressortweiten IT-Sicherheitsmaßnahmen,
- ✗ die Planung und Koordinierung von Schulungs- und Sensibilisierungsmaßnahmen, in Bezug auf IT-Sicherheit,
- ✗ die Stärkung des Bewusstseins für IT-Sicherheit im Managementbereich,
- ✗ die Einbringung von IT-Sicherheitsprojektanträgen in das SIT.

Er stellt im IT-Sicherheitsmanagementteam die Ansprechstelle für alle am IT-Sicherheitsmanagementprozess beteiligten Personen (Führungspersonal, SIT, IT-Sicherheitsorganisationsstruktur, usw.) dar.

5.4.2 IT-Sicherheitsmanagement-Team (IST)

Das IT-Sicherheitsmanagement-Team setzt sich aus folgenden gleichrangigen, ständigen Mitgliedern zusammen:

- ✗ dem Informationssicherheitsbeauftragten des BMI
(Entsprechend §7 des Informationssicherheitsgesetzes InfoSiG sind für jedes Bundesministerium ein Informationssicherheitsbeauftragter und dessen Stellvertreter zu bestellen.)

Seine Aufgaben und Pflichten sind im InfoSiG bzw. in der Informationssicherheitsverordnung InfoSiV definiert.),

- ✗ dem Datenschutzbeauftragten des BMI
(Die Funktion des Datenschutzbeauftragten wird in dem durch die Ressortleitung unterfertigten Datenschutzerlass festgelegt. Der Datenschutzbeauftragte und sein Stellvertreter kommen aus dem laut der Geschäftseinteilung des BMI unmittelbar für die konzeptiven Belange des Datenschutzes zuständigen Organisationsbereich),
- ✗ optional einem Kommunikationsverantwortlichen
(Sollte innerhalb des Ressorts die Notwendigkeit nach einer Regelung des inter- und intraministeriellen, sowie nationalen und internationalen Informationsaustausches durch einen eigenen Kommunikationsverantwortlichen bestehen und diese Rolle etabliert werden, wäre dieser auch als ständiges Mitglied des IT-Sicherheitsmanagementteams aufzunehmen.),
- ✗ dem Chief Information Officer (CIO) des BMI
(Durch diesen bzw. seinen Stellvertreter sollen alle die IT-Sicherheit betreffenden Belange des primären IT-Serviceanbieters und –Dienstleiters des BMI vertreten werden. Weiters stellt der CIO die Schnittstelle zum IKT-Board dar.),
- ✗ dem IT-Sicherheitsbeauftragten.

Zusätzlich kann das IT-Sicherheitsmanagementteam bei Bedarf interne und externe Berater für seine ihm übertragenen Tätigkeiten heranziehen, bzw. die Bereichs-IT-Sicherheitsbeauftragten in das Team berufen.

Für das IT-Sicherheitsmanagement-Team ist eine Geschäftsordnung zu erstellen, welche die Zuständigkeiten innerhalb des Teams, sowie die Verantwortlichkeiten gegenüber dem SIT und die Kommunikations- und Entscheidungswege festlegt.

Das IT-Sicherheitsmanagement-Team kann zur Erfüllung der ihm übertragenen Aufgaben auch auf die Ressourcen des laut der Geschäftseinteilung des BMI explizit für die IT-Sicherheit zuständigen Organisationsbereiches zurückgreifen.

Das IT-Sicherheitsmanagement-Team ist im Rahmen des IT-Sicherheitsmanagementprozesses für folgende Belange der IT-Sicherheit ressortweit zuständig:

- ✗ Entwicklung und laufende Aktualisierung der ressortweiten IT-Sicherheitspolitik,
- ✗ Festlegung einer Risikoanalysestrategie und Erstellung von Risikoanalysen,
- ✗ Erstellung und laufende Aktualisierung eines IT-Sicherheitskonzeptes:

- In Abhängigkeit der Ergebnisse der Risikoanalysen sind Vorschläge für Maßnahmen zu erstellen, die die Risiken auf ein beherrschbares und tragbares Ausmaß reduzieren sollen. Dazu wird das verbleibende Restrisiko ermittelt.
- Um die resultierenden IT-Sicherheitspläne überschaubar zu halten, sind für einzelne Bereiche zur ressortweiten IT-Sicherheitspolitik kompatible IT-Systemsicherheitspolitiken zu entwickeln.
- Für die einzelnen IT-Sicherheitspolitiken sind IT-Sicherheitspläne zu erstellen, die alle kurz-, mittel- und langfristigen erforderlichen Aktionen festhalten die für die Umsetzung der vorgeschlagenen Maßnahmen notwendig sind.
- ✍ Ausarbeitung von Maßnahmen zur Förderung des IT-Sicherheitsbewusstseins innerhalb des gesamten Ressorts,
- ✍ Überprüfung der gesteckten IT-Sicherheitsziele auf ihre Erreichung,
- ✍ Verwaltung der für die IT-Sicherheit zur Verfügung stehenden Ressourcen für die Umsetzung kurzfristig notwendiger Maßnahmen.

Dies erfordert aber auch, dass

- ✍ definierte personelle und finanzielle Ressourcen für die Aufrechterhaltung des IT-Sicherheitsmanagementprozesses bereitgestellt werden,
- ✍ technische und organisatorische Sicherheits- und Kontrollmaßnahmen festgelegt werden und deren Einführung unterstützt wird,
- ✍ die Wirksamkeit der gesetzten IT-Sicherheitsmaßnahmen regelmäßig durch geeignete Penetrationsversuche überprüft wird.

Das IT-Sicherheitsmanagement-Team berichtet regelmäßig der Ressortleitung und dem SIT über den Stand der Informationssicherheit.

5.4.3 IST-Büro

Die administrative Betreuung für das IST wird von dem laut Geschäftseinteilung des BMI explizit für die IT-Sicherheit zuständigen und mit entsprechenden Ressourcen ausgestatteten Organisationsbereich wahrgenommen. Dem Büro des IST kommen folgende Aufgaben zu:

- ✍ Vorbereitung der Sitzungen des IST, insbesondere
 - die Ausarbeitung von IT-Sicherheitsrichtlinien
 - die Ausarbeitung von IT-Sicherheitsprojektanträgen

- die Ausarbeitung der IT-Sicherheitsberichte
- ✗ die Präsentation von IT-Sicherheitsthemen im BMI-Intranet
- ✗ die Verwaltung der für die IT-Sicherheit zur Verfügung stehenden Ressourcen für die Umsetzung kurzfristig notwendiger Maßnahmen gemäß den Vorgaben des IST

5.4.4 Bereichs IT-Sicherheitsbeauftragte

Die Bereichs-IT-Sicherheitsbeauftragten werden jeweils von dem für die Sektion zuständigen BIT vorgeschlagen und vom SIT eingesetzt. Pro Sektion ist zumindest ein verantwortlicher Bereichs-IT-Sicherheitsbeauftragter zu bestellen.

Alle Bereichs IT-Sicherheitsbeauftragten sind mit fachgebundener Weisungsbefugnis ausgestattet und steuern die Einführung und die Umsetzung der Regelungen zur IT-Sicherheit in ihrem Verantwortungsbereich. Sie stellen insbesondere sicher, dass

- ✗ das Bewusstsein für IT-Sicherheit bei den Mitarbeitern gestärkt wird,
- ✗ die Informationssysteme des eigenen Bereiches ausreichend geschützt sind und entsprechend der gültigen Regelungen zur IT-Sicherheit betrieben und genutzt werden,
- ✗ eine aktuelle, vollständige und entsprechend detaillierte Dokumentation der im eigenen Bereich implementierten IT-Sicherheitsmaßnahmen vorhanden ist,
- ✗ das IST dabei unterstützt wird, Sicherheitslücken – insbesondere im organisatorischen Bereich – umgehend zu beseitigen bzw. Analysen und Prüfungen durchzuführen zu lassen.

Darüber hinaus unterstützen die Bereichs-IT-Sicherheitsbeauftragten die Weiterentwicklung des IT-Sicherheitsmanagementprozesses in ihrem Verantwortungsbereich aber auch ressortweit, jeweils in Zusammenarbeit mit dem IT-Sicherheitsmanagement-Team. Dies erfordert, dass sie

- ✗ bei der Entwicklung und der Einführung von ressortweiten und sektions- oder bereichsspezifischen Regelungen und Programmen zur IT-Sicherheit mitarbeiten,
- ✗ bei der Vorbereitung und Durchführung von Trainingsprogrammen zur IT-Sicherheit mitwirken,
- ✗ die Mitarbeiter in ihrem Zuständigkeitsbereich bei der Einführung von Maßnahmen zur IT-Sicherheit beraten und unterstützen.

Das Tätigkeitsprofil ist in die jeweilige Arbeitsplatzbeschreibung aufzunehmen und der daraus resultierende prozentuelle Arbeitsaufwand festzulegen. Hierbei ist festzuhalten, dass dadurch keine Konkurrenz zu den bestehenden BIT-Strukturen des Ressorts geschaffen wird. Die Tätigkeiten der

Bereichs-IT-Sicherheitsbeauftragten beschränken sich ausschließlich auf IT-sicherheitsrelevante – und hier insbesondere organisatorische – Themenkreise. Umgekehrt ist nicht ausgeschlossen, dass Mitarbeiter von BIT´s auch die Rolle von Bereichs- IT-Sicherheitsbeauftragten übernehmen können.

Die Bereichs IT-Sicherheitsbeauftragten berichten dem IT-Sicherheitsmanagement-Team regelmäßig über den Stand der IT-Sicherheit und melden wesentliche Schwachstellen und Vorfälle unverzüglich dem IT-Sicherheitsbeauftragten.

5.4.5 System IT-Sicherheitsbeauftragte

Die Komplexität der im BMI im Einsatz befindlichen Informationssysteme erfordert zur Gewährleistung eines angemessenen Sicherheitsniveaus tief gehende Systemkenntnisse, die von einer einzelnen Person nicht mehr umfassend über alle eingesetzten Systemplattformen hinweg abgedeckt werden können.

Als Systeme in diesem Sinne können z.B. die BAKS-Infrastruktur (Büroautomations- und Kommunikationssystem Plattform), das Zentralsystem (EKIS/FIS/SIS), das Kommunikationssystem des BMI, das BMI-Netz, usw. angesehen werden.

Die jeweils aktuellen System-Sicherheitsbereiche werden vom IT-Sicherheitsmanagementteam festgelegt und die dazugehörigen Sicherheitsbeauftragten in Abstimmung mit der für den Betrieb des jeweiligen Systems verantwortlichen Organisationseinheit definiert.

Zu den Aufgaben eines System IT-Sicherheitsbeauftragten zählen

- ✍ die Mitwirkung bei den seinen Bereich betreffenden Teilen des IT-Sicherheitskonzepts,
- ✍ die Erarbeitung eines detaillierten Planes zur Realisierung der ausgewählten IT-Sicherheitsmaßnahmen,
- ✍ die Umsetzung dieses Planes,
- ✍ eine aktuelle, vollständige und entsprechend detaillierte Dokumentation der im eigenen Bereich implementierten IT-Sicherheitsmaßnahmen,
- ✍ die regelmäßige Prüfung der Wirksamkeit und Einhaltung der eingesetzten IT-Sicherheitsmaßnahmen im laufenden Betrieb,
- ✍ Information des IT-Sicherheitsbeauftragten über bereichsspezifischen Schulungsbedarf, sowie

- ✗ unverzügliche Meldung von erkannten Schwachstellen bzw. sicherheitsrelevanten Ereignissen an den IT-Sicherheitsbeauftragten.

Das Tätigkeitsprofil ist in die jeweilige Arbeitsplatzbeschreibung aufzunehmen und der daraus resultierende prozentuelle Arbeitsaufwand festzulegen.

5.4.6 IT-Sicherheitsvertrauenspersonen (ISV)

Um Maßnahmen zur IT-Sicherheit flächendeckend umzusetzen, werden freiwillige und speziell geschulte Mitarbeiter als Vertrauenspersonen etabliert, die

- ✗ andere Mitarbeiter bezüglich IT-Sicherheit sensibilisieren,
- ✗ andere Mitarbeiter bei der Anwendung von Richtlinien zur IT-Sicherheit unterstützen,
- ✗ die sicherheitsrelevanten Zusammenhänge ihres Umfeldes aktiv kennen lernen sollen,
- ✗ Informationen über mögliche Schwachstellen der IT-Sicherheit an den Bereichs-IT-Sicherheitsbeauftragten melden,
- ✗ helfen, konkrete Vorfälle mit Auswirkung auf die IT-Sicherheit zu identifizieren und korrekt an den Helpdesk der Abteilung IT-MS zu melden,
- ✗ regelmäßig an Fortbildungsmaßnahmen zu Themen der IT-Sicherheit teilnehmen und die aktuellen Informationen zur IT-Sicherheit im Intranet durcharbeiten.

5.5 Applikations- und Projektverantwortliche

Die Verantwortlichen für den Betrieb von Anwendungen stellen sicher, dass diese für die jeweiligen Anwender rechtzeitig, korrekt und sicher nutzbar sind. Dies erfordert, dass

- ✗ der Zugriff auf Informationssysteme zur Nutzung, Administration, Wartung und zu anderen Zwecken nur durch Berechtigte erfolgt (Definition von Rollen und Zuordnung von Zugriffsrechten),
- ✗ der Zugriff auf Informationen, die in Informationssystemen gespeichert, verarbeitet oder übertragen werden, nur für Berechtigte möglich ist (Klassifikation von Informationen und Vergabe von Zugriffsrechten),
- ✗ der berechtigte Zugriff auf die in den IT-Systemen abgelegten Informationen innerhalb eines definierten Zeitraumes ermöglicht wird (Festlegung von Verfügbarkeitsklassen)
- ✗ die Voraussetzungen für die regelmäßige Überprüfung von Zugriffen geschaffen werden (Protokollierung)

- ✗ Informationssysteme regelmäßig auf Schwachstellen und die Einhaltung der gültigen Regelungen zur IT-Sicherheit überprüft werden,
- ✗ Anwender bei Bedarf auf bekannte Schwachstellen und deren Vermeidung aufmerksam gemacht werden,
- ✗ der IT-Sicherheitsbeauftragte des Ressorts umgehend über nicht behebbare Schwachstellen, wesentliche Vorfälle oder sicherheitsrelevante Veränderungen informiert wird.

Für jedes relevante Informationssystem, IT-Anwendung und IT-Projekt ist die Verantwortung für die IT-Sicherheit bereits vor dem Einsatz klar festzulegen. Ebenso sind die Aufgaben und Verantwortlichkeiten von IT-Entwicklung, technischen Support (inklusive Userverwaltung), Dienstnehmer, Leasingpersonal, externer Mitarbeiter, Lieferanten und Vertragspartner im Detail zu definieren.

IT-Dienstleistungen dürfen auch an externe Dienstleister delegiert werden, jedoch muss hierfür im BMI ein Projektverantwortlicher existieren, der seine Kontrollpflichten auf den externen Dienstleister ausdehnt. Die relevanten IT-Sicherheitsrichtlinien sind schriftlich in einem Service Level Agreement vertraglich zu vereinbaren und dürfen nicht im Gegensatz zu den Grundsätzen der IT-Sicherheitspolitik und den nachgeordneten Richtlinien stehen.

5.6 Mitarbeiter

Alle Mitarbeiter des Ressorts sind verpflichtet, die Sicherheit von Informationen und Informationssystemen, auf die sie Zugriff haben, zu wahren und aktiv zu fördern. Dies erfordert, dass

- ✗ Informationen und Informationssysteme ausschließlich im Sinne der zugewiesenen Aufgaben genutzt werden,
- ✗ angemessene Sorgfalt beim Umgang mit diesen Informationen gewahrt wird,
- ✗ ausschließlich Informationssysteme, Komponenten und Anwendungen (Software) benutzt werden, die vom Dienstgeber zur Verfügung gestellt werden, bzw. durch den Dienstgeber akkreditiert wurden,
- ✗ die gültigen Regelungen zur IT-Sicherheit eingehalten werden,
- ✗ ggf. zusammen mit dem Vorgesetzten für wichtige und sensible Informationen der Grad der Vertraulichkeit und Sensibilität festgelegt wird und die damit verbundenen Richtlinien und Gesetze eingehalten werden,
- ✗ Schwachstellen einer IT-Sicherheitsvertrauensperson bekannt gemacht werden,
- ✗ Vorfälle mit Auswirkung auf die IT-Sicherheit unverzüglich an IT-Sicherheitsvertrauensperson bzw. den Helpdesk der Abteilung IT-MS gemeldet werden.

6 Risikostrategien, Restrisiko und Risikoakzeptanz

Methodisches Risikomanagement ist zur Erarbeitung eines vollständigen und organisationsweiten Sicherheitskonzeptes unerlässlich. Um Risiken zu beherrschen ist es zunächst erforderlich, sie zu kennen und zu bewerten. Je nach der in der Risikoanalyse angewandten Methodik drückt sich das Risiko als eine Menge identifizierter fehlender Maßnahmen oder in einem möglichen Schadensbetrag multipliziert mit der Wahrscheinlichkeit des Auftretens aus. Dazu wird in einer Risikoanalyse das Gesamtrisiko ermittelt. Ziel ist es, mit Hilfe von zusätzlichen Maßnahmen dieses Risiko so weit zu reduzieren, dass das verbleibende Restrisiko quantifizierbar und akzeptierbar wird.

Auch bei Durchführung aller ausgewählten Sicherheitsmaßnahmen verbleibt immer ein Restrisiko, dessen Abdeckung wirtschaftlich nicht mehr vertretbar wäre. Verbleibt nach Durchführung aller im Sicherheitsplan vorgesehenen Maßnahmen ein Restrisiko, dessen weitere Reduktion nicht möglich oder unwirtschaftlich wäre, so besteht die Möglichkeit einer bewussten Akzeptanz des Restrisikos.

Je früher die IT-Sicherheit im Lebenszyklus eines Informationssystems oder einer IT-Anwendung berücksichtigt wird, desto geringer sind die hierfür anfallenden Kosten. Deshalb ist eine Risikoanalyse schon bei der Planung, Entwicklung bzw. Inbetriebnahme eines neuen IT-Systems vorzunehmen, um die notwendige Sicherheit im laufenden Betrieb durch angemessene Maßnahmen gewährleisten zu können.

Die Ergebnisse der IT-Risikoanalyse sollen dazu dienen, die ressortspezifischen Schutzbedürfnisse herauszuarbeiten und das Volumen bzw. die Priorisierung der notwendigen IT-Sicherheitsmaßnahmen für das IT-Sicherheitskonzept in angemessener Weise zu steuern.

Bezüglich der Analysemethode wird der kombinierte Ansatz als Risikoanalysestrategie festgelegt. Diese Vorgehensweise kombiniert die Vorteile des Grundschutzansatzes, sowie jene einer detaillierten Risikoanalyse, da alle IT-Systeme mit hohem Schutzbedarf wirksam und angemessen geschützt werden. Systeme mit geringerem Schutzbedarf werden mit Hilfe von vordefinierten Grundschutzmaßnahmen schnell und effektiv abgesichert.

In einem ersten Schritt wird in der Schutzbedarfsfeststellung (High Level Risk Analysis) der Schutzbedarf für die einzelnen IT-Systeme ermittelt. Für Systeme der Schutzbedarfskategorie „niedrig bis mittel“ wird auf eine detaillierte Risikoanalyse verzichtet. Dies erlaubt eine schnelle und effektive Auswahl von grundlegenden Sicherheitsmaßnahmen bei gleichzeitiger Gewährleistung eines angemessenen Schutzniveaus.

IT-Systeme der Schutzbedarfskategorie „sehr hoch“ sind sofort einer detaillierten IT-Risikoanalyse zu unterziehen, damit möglichst schnell angemessene Maßnahmen zur Risikobegrenzung ergriffen werden, mit dem Ziel, möglichen Krisen zuvorzukommen.

IT-Systeme mit Schutzbedarf „hoch“ sind nachfolgend ebenfalls einer detaillierten IT-Risikoanalyse zu unterziehen.

Nach der Durchführung der Risikoanalyse unterbreitet das IT-Sicherheitsmanagement-Team dem SIT die Faktenlage bezüglich der vorgefundenen Schwachstellen und Verbesserungspotentiale, wobei Schwachstellen mit vertretbarem Restrisiko keiner sofortigen weiteren Maßnahmen bedürfen.

In einem nachfolgenden durch das IST auszuarbeitenden Sicherheitskonzept werden die Maßnahmen im Detail ermittelt, welche zur Beherrschung der Risiken insgesamt erforderlich sind. Hierbei werden die Aufwände und Kosten im Einzelnen ermittelt, und es erfolgt die Auswahl von Maßnahmen, die nachfolgend realisiert werden sollen. Das Restrisiko entsteht, weil es in der Regel aus technischen, organisatorischen oder wirtschaftlichen Gründen nicht möglich ist, alle Sicherheitsmaßnahmen unverzüglich umzusetzen. Außerdem verringern Maßnahmen die Schadenshöhe und Eintrittswahrscheinlichkeit niemals zur Gänze.

Sollte das SIT oder die Leitung des Ressorts das Restrisiko nicht akzeptieren, sind von ihnen zu verantwortende Maßnahmen einzuleiten (z. B. die Änderung der Sicherheitspolitik, das Heranziehen externer Sachverständiger, eine Erhöhung des IT-Sicherheitsbudgets), um eine Lösung mit akzeptablem Restrisiko zu erreichen.

Die Akzeptanz des Restrisikos wird durch das Vorhandensein einer Disaster Recovery Planung erhöht. Für den Fall, dass ein Restrisiko durch eine Notfallmaßnahme abgedeckt wird, kann es im Sinne der Grundsätze zur IT-Sicherheitspolitik jedenfalls akzeptiert werden.

7 Maßnahmen zur IT-Sicherheit

Um das Risiko im Sinne der IT-Sicherheit erfolgreich zu reduzieren, sind verpflichtende Richtlinien und Maßnahmen erforderlich. Sie dienen dazu, um die Wahrscheinlichkeit eines Schadenseintrittes oder den möglichen Schadensbetrag zu reduzieren.

Die Klassifizierung der von den Informationssystemen verarbeiteten Daten in Bezug auf Vertraulichkeit, Datenschutz, Integrität und Verfügbarkeit ist eine wesentliche Voraussetzung für die Auswahl von Sicherheitsrichtlinien und –maßnahmen.

Die angemessene Klassifizierung und Handhabung von Informationen wird in einer gesonderten IT-Sicherheitsrichtlinie im Detail beschrieben und allen Mitarbeitern als Arbeitsgrundlage zur Kenntnis gebracht.

7.1 Klassifizierung von Informationen und IT-Anwendungen

In Bezug auf *Vertraulichkeit* gibt es entsprechend dem InfoSiG und der InfoSiV vier Klassen mit unterschiedlichen Handhabungsvorschriften für wichtige Informationen:

- ✍ Klasse E „eingeschränkt“: wenn die unbefugte Weitergabe den in Art. 20 Abs. 3 B-VG genannten Interessen zuwider laufen würde (z. B.: behördeninterner Schriftverkehr, interne Telefonverzeichnisse, Organisationspläne, alle nicht klassifizierten Informationen),
- ✍ Klasse V „vertraulich“: wenn die Informationen unter strafrechtlichem Geheimhaltungsschutz stehen und ihre Geheimhaltung im öffentlichen Interesse gelegen ist,
- ✍ Klasse G „geheim“: wenn die Informationen vertraulich sind und ihre Preisgabe zudem die Gefahr einer erheblichen Schädigung der in Art. 20 Abs. 3 B-VG genannten Interessen schaffen würde,
- ✍ Klasse SG „streng geheim“: wenn die Informationen geheim sind und überdies ihr Bekanntwerden eine schwere Schädigung der in Art. 20 Abs. 3 B-VG genannten Interessen wahrscheinlich machen würde.

Für Informationen die ausdrücklich für die Veröffentlichung freigegeben wurden, gilt zusätzlich die

- ✍ Klasse O „offen“: z.B.: Gesetze, Verordnungen, Pressemitteilungen

Bei der Klassifizierung nach der *Vertraulichkeit* ist entsprechende Sorgfalt notwendig, da eine zu niedrige Einstufung mit der Gefahr des Missbrauches bzw. eine zu hohe Einstufung mit einem nicht zu rechtfertigenden Aufwand verbunden ist.

In Bezug auf *Datenschutz* gibt es aus dem DSG abgeleitet ebenfalls vier *Sensibilitätsklassen* für Informationen mit jeweils unterschiedlichen Handhabungsvorschriften:

- ✍ Klasse N „nicht personenbezogene Informationen“: Alle Informationen die nicht unter die §8 und 9 DSG zu subsumieren sind.
- ✍ Klasse P „personenbezogene, nicht sensible Daten“: Alle Informationen die unter §8 Abs. 1-3 DSG zu subsumieren sind.
- ✍ Klasse ST „personenbezogene Daten mit strafrechtlichem Inhalt“: Alle Informationen die unter §8 Abs. 4 DSG zu subsumieren sind.
- ✍ Klasse S „sensible personenbezogene Daten“: Alle Informationen die unter §9 DSG zu subsumieren sind.

Alle Informationen sind unbedingt sowohl im Hinblick auf *Vertraulichkeit* als auch bezüglich *Sensibilität* zu klassifizieren. Die Klassifizierung hat prinzipiell durch den zuständigen Sachbearbeiter, in Ausnahmefällen mit dem Informationssicherheitsbeauftragten oder dem Datenschutzbeauftragten, zu erfolgen. Alle dem BMI zukommenden, bzw. durch das BMI verarbeiteten Informationen müssen durch die in der Sicherheitspolitik für das BMI festgelegten Klassen klassifiziert werden. Erlangt ein Mitarbeiter ursprünglich nicht oder nur unzureichend klassifizierte Informationen, bzw. entspricht die Einstufung nicht den im BMI verwendeten Klassen, so hat die Erstklassifizierung bzw. die Zuordnung zu den im BMI gültigen Klassen durch ihn zu erfolgen. Aufgrund von EU-Recht, dem InfoSiG bzw. DSG klassifizierte Dokumente dürfen dabei durch Mitarbeiter des BMI jeweils nur in eine höhere Klasse umgestuft werden. Eine Rückstufung solcher Informationen kann nur durch bzw. in Abstimmung mit den Informationsproduzenten bzw. Informationslieferanten erfolgen. Prinzipiell ist jede Umstufung entsprechend zu dokumentieren.

Generell gilt für das gesamte Ressort, dass die Klassifikation nicht oder unzureichend eingestufte Informationen mit der *Vertraulichkeit* „eingeschränkt“ und/oder der *Sensibilität* „personenbezogene, nicht sensible Daten“ ergänzt wird.

Für die *Verfügbarkeit* von IT-Anwendungen werden z. B. für die Disaster Recovery Planung weitere Klassen definiert, um die Abhängigkeit des Geschäftsprozesses von der Information oder dem Informationssystem zu charakterisieren und ermöglichen, angemessene Maßnahmen zu ihrem Schutz zu ergreifen.

Um den Verfügbarkeitsanspruch von IT-Anwendungen im Ressort darstellen zu können, werden folgende der IKT-Strategie des Bundes entsprechende Verfügbarkeitsklassen definiert:

- ✎ Verfügbarkeitsklasse 1 (Keine Vorsorge / unkritisch): Für die IT-Anwendung werden keine besonderen Vorkehrungen getroffen. Datenverlust bzw. Ausfall der IT-Anwendung auf unbestimmte Zeit ist denkbar. Eine Behinderung der Wahrnehmung der Aufgaben der betroffenen Organisationseinheiten entsteht dadurch nicht oder nur in einem akzeptablen Ausmaß.
- ✎ Verfügbarkeitsklasse 2 (Offline Sicherung): Es sind gängige Sicherungsmaßnahmen für die IT-Anwendung vorgesehen, ein Datenverlust ist auszuschließen. Die IT-Anwendung kann bei technischen Problemen erst nach deren Behebung am ursprünglichen Produktionssystem in Betrieb genommen werden. Die Sicherung wird an einem externen Ort ausgelagert.
- ✎ Verfügbarkeitsklasse 3 (Redundante Infrastruktur): Die Infrastruktur für die IT-Anwendung ist derart ausgelegt, dass bei Ausfall einer IT-Komponente der Betrieb durch redundante Auslegung ohne Unterbrechung fortgesetzt werden kann.
- ✎ Verfügbarkeitsklasse 4 (Redundanter Standort): Die IT-Infrastruktur sowie die darauf aufsetzende IT-Anwendung ist auf zwei oder mehrere Standorte verteilt, so dass bei Betriebsunterbrechung eines Standortes, die IT-Anwendung uneingeschränkt an einem anderen Standort weiter betrieben werden kann.

Für die Verfügbarkeitsklassen 2 – 4 kann noch das zusätzliche Qualitätsmerkmal „K“ (für „Kfall sicher“) gemäß der Katastrophenvorsorgestrategie des Bundes definiert werden. Daraus resultieren entsprechende Maßnahmen die zumindest einen Notbetrieb in einer „Zero-Risk- Umgebung“ gewährleisten.

Für IT-Anwendungen des Ressorts erfolgt die Klassifizierung durch die Projekt- bzw. Applikationsverantwortlichen. Grundsätzlich ist zumindest die *Verfügbarkeitsklasse 2* anzustreben. Ist jedoch für eine IT-Anwendung keine Einstufung vorhanden, wird automatisch von der *Verfügbarkeitsklasse 1* ausgegangen.

7.2 Integrität von Daten und Informationssystemen

Informationen sollten, abhängig von einer Risikoanalyse, mit der maximal erreichbaren Integrität zur Verfügung gestellt werden. Hierfür sind entsprechende technische und organisatorische Maßnahmen (Message Authentication Codes, Digitale Signaturen, Prüf- und Kommunikationsprotokolle, Vermeidung von Viren und trojanischen Pferden, Backup-Konzepte) einzusetzen.

7.3 Organisationsweite Richtlinien zu Sicherheitsmaßnahmen

Folgende, beispielsweise angeführten, organisationsweiten Richtlinien dokumentieren im Detail die erforderlichen Sicherheitsmaßnahmen. Diese Informationen machen die Verantwortlichkeiten in der Praxis deutlich und unterstützen den Anwender, die Personalabteilung, IT-Sicherheits-, System-, Applikations- und Projektverantwortlichen durch detaillierte, zielgruppenorientierte Anleitungen.

Zielgruppe: Mitarbeiter

- ✗ IT-Sicherheitsrichtlinie zur Klassifizierung und Handhabung von Informationen
- ✗ IT-Sicherheitsrichtlinie zur Verantwortung und IT-Sicherheit am Arbeitsplatz und Erläuterung der Konsequenzen bei Zuwiderhandeln
- ✗ Erlass zur Regelung der elektronischen Kommunikation mittels e-Mail
- ✗ Erlass zur Regelung des Internetzuganges des Ressorts
- ✗ IT-Sicherheitsrichtlinie zum Incident Handling
- ✗ IT-Sicherheitsrichtlinie zur Nutzung von mobilen IT-Geräten

Zielgruppen: IT-Sicherheitsverantwortliche und Verantwortliche des IKT-Betriebes

- ✗ IT-Sicherheitsrichtlinie zur Zugriffskontrolle
- ✗ IT-Sicherheitsrichtlinie zur Protokollierung
- ✗ IT-Sicherheitsrichtlinie zur Archivierung
- ✗ IT-Sicherheitsrichtlinie zur Datensicherung
- ✗ IT-Sicherheitsrichtlinie zum Virenschutz
- ✗ IT-Sicherheitsrichtlinie zur Aufstellung, Installation, Wartung, Reparatur und Außerbetriebnahme von Informationssystemen
- ✗ IT-Sicherheitsrichtlinie zur Netzwerksicherheit
- ✗ IT-Sicherheitsrichtlinie zur Softwarenutzung und –entwicklung

Zielgruppe: Personalabteilung

- ✗ IT-Sicherheitsrichtlinie zur personellen Sicherheit

Die für die Zielgruppe „Mitarbeiter“ erstellten Richtlinien werden zusammen mit den Grundsätzen zur IT-Sicherheitspolitik in einem IT-Sicherheitsinformationssystem im Intranet allen Mitarbeitern des Ressorts bekannt und zugänglich gemacht.

7.4 Disaster Recovery Planung

Ziel der Disaster Recovery Planung ist es, die Verfügbarkeit der wichtigsten Applikationen und Systeme innerhalb eines definierten Zeitraumes zu gewährleisten, sowie Vorkehrungen zur Schadensbegrenzung im Katastrophenfall zu treffen.

Entsprechend der Definition der Verfügbarkeitsklassen wird ein angemessener Aufwand zur Wiederherstellung von Daten, Applikationen und Informationssystemen gerechtfertigt.

In einer Notfallanalyse werden nur im wirtschaftlichen Rahmen vertretbare Notfallbehandlungen in die Disaster Recovery Planung aufgenommen. Das Restrisiko (Ausfall wesentlicher Geschäftsprozesse des BMI im Katastrophenfall) muss von der Leitung des Ressorts getragen werden.

Diese Notfallanalyse sollte schon bei der Planung, Entwicklung bzw. Inbetriebnahme eines relevanten neuen IT-Systems vorgenommen werden, um durch Maßnahmen im laufenden Betrieb (z.B. Backup-Konzept), die Schadensbegrenzung im Notfall zu gewährleisten.

In diesem Backup-Konzept ist dafür zu sorgen, dass regelmäßige Sicherungen aller für den Geschäftsablauf notwendigen Informationen durchgeführt werden und entsprechend ihrer Klassifizierung nach Eintritt eines Notfalles wieder verfügbar werden.

Die detaillierte Disaster Recovery Planung wird gesondert beschrieben und ist der Abteilung IT-MS, den System-, den Applikations- und den IT-Sicherheitsverantwortlichen zur Kenntnis zu bringen.

7.5 Nachfolgeaktivitäten zur Überprüfung und Aufrechterhaltung der IT-Sicherheit

Ein IT-Sicherheitskonzept ist kein statisches, unveränderliches Dokument, umfassendes IT-Sicherheitsmanagement beinhaltet vielmehr die Aufgabe, IT-Sicherheit in einer sich ständig wandelnden Betriebsumgebung aufrecht zu erhalten.

Zur Aufrechterhaltung des erreichten Sicherheitslevels ist es erforderlich, dass

- ✍️ Wartung und administrativer Support der Sicherheitseinrichtungen gewährleistet wird,
- ✍️ die realisierten Maßnahmen regelmäßig auf Ihre Übereinstimmung mit der Sicherheitspolitik und den nachgeordneten Richtlinien geprüft werden (Security Compliance Checking),
- ✍️ die IT-Systeme fortlaufend überwacht werden (Monitoring).

Die System- und Applikationsverantwortlichen überwachen die sicherheitsrelevanten Änderungen und eskalieren die entstehenden Sicherheitsprobleme umgehend an den IT-Sicherheitsbeauftragten des Ressorts. Dieser initiiert innerhalb des IT-Sicherheitsmanagement- Teams die Anpassung der relevanten Richtlinien und gegebenenfalls die Einführung neuer Sicherheitsmaßnahmen (Change Management).

Risikoveränderungen werden unter anderem auch durch die IT-Sicherheit betreffende Vorfälle sichtbar. Die erforderlichen Rollen, Aufgaben und Verantwortlichkeiten für das Incident Handling ergeben sich aus dem Kapitel „Verantwortlichkeiten und Pflichten“ und werden im Detail in den IT-Sicherheitsrichtlinien beschrieben.

7.6 IT-Sicherheitsdokumentation des BMI

Die detaillierte Beschreibung aller aktuellen organisatorischen, personellen, infrastrukturellen und technischen IT-Sicherheitsmaßnahmen wird in einer umfassenden und vollständigen Sammlung in Form eines IT-Sicherheitshandbuches des BMI dokumentiert und über den gesamten System-Lifecycle fortgeschrieben.

Das IT-Sicherheitshandbuch des BMI ist als „*vertraulich*“ und „*nicht personenbezogen*“ klassifiziert und steht in seiner Gesamtheit nur der Ressortleitung, den Mitgliedern des SIT und den Mitgliedern des IST zur Einsicht zur Verfügung.

Die für einzelne IT-Sicherheitsbereiche, IT-Systeme und Applikationen spezifischen Informationen, werden in geeigneter Weise auch den jeweils verantwortlichen Bereichs- und System- IT-Sicherheitsbeauftragten sowie Applikationsverantwortlichen zur Verfügung gestellt.

8 Life Cycle der IT-Sicherheitspolitik

Die Grundsätze zur IT-Sicherheitspolitik werden von der Leitung des Ressorts offiziell verabschiedet und in Kraft gesetzt.

Es ist die Aufgabe aller Managementebenen, eine sichtbare Unterstützung für die erfolgreiche Implementierung und Umsetzung der IT-Sicherheitspolitik zu geben und ihre vorgesehenen Rollen bzgl. der in diesem Dokument definierten Verantwortlichkeiten auszufüllen.

Der IT-Sicherheitsverantwortliche des Ressorts erhält die Funktion des Process Owners für die IT-Sicherheitspolitik und wird hierzu von der Leitung des Ressorts beauftragt. Diese Grundsätze sind im Bedarfsfall, mindestens jedoch alle 2 Jahre auf Aktualität und Wirksamkeit zu überprüfen, einer Überarbeitung zuzuführen und im Ressort neu abzustimmen.

Wien, 1. September 2003