# IT-SICHERHEITSMANAGEMENT

## Sicherheit, Integrität, Vertraulichkeit

***Das Bundesministerium für Inneres hat seine IT-Sicherheitspolitik auf den neuesten Stand gebracht. In der ersten Phase des IT-Sicherheitsmanagement-Prozesses wurde das Grundsatzdokument "IT-Sicherheit – Grundsätze zur IT-Sicherheitspolitik des BM.I" erarbeitet.***

Das Bundesministerium für Inneres (BM.I) hat den Auftrag, die innere Sicherheit dieses Landes zu gewährleisten und zukunftsweisend auszubauen. Es ist das größte und sensibelste Dienstleistungsunternehmen im Bereich Sicherheit; seine Arbeit wird immer mehr vom Einsatz moderner Informationstechnologie (IT) bestimmt. Der ungestörte Ablauf der Geschäftsprozesse und das Image des Ressorts sind 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.

Das Thema Informationssicherheit hat in den letzten Jahren zunehmend internationale Organisationen beschäftigt. Die Europäische Kommission hat in ihrer Mitteilung Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz (Juni 2001) die Wichtigkeit dieses Problems hervorgehoben. Die Kommission empfiehlt den Mitgliedstaaten, beispielhafte Maßnahmen wie 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 sind in Österreich mit dem Strafrechtsänderungsgesetz 2002 unter anderem neue Straftatbestände geschaffen worden, auch in Umsetzung der Cybercrime-Konvention des Europarats vom November 2001 – z.B. "Widerrechtlicher Zugriff auf ein Computersystem", "Störung der Funktionsfähigkeit eines Computersystems", "Missbräuchliches Abfangen von Daten" oder "Datenfälschung".

Veränderungen im Bereich der Organisationsstruktur des Ressorts, die Konsolidierung des ressortweiten Büroautomations- und Kommunikationssystems (Baks), auch der dramatisch ansteigende – internetbasierende – Kommunikationsbedarf im Rahmen der aktuellen und zukünftigen E-Government-Präsenz des Innenministeriums, haben eine umfassende Überarbeitung und Neugestaltung des IT-Sicherheitsmanagement-Prozesses notwendig gemacht.

## Strategie und Ziele

Ziel der IT-Sicherheit im BM.I ist es, alle für die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung notwendigen Informationen rechtzeitig, korrekt und sicher dem berechtigten Personenkreis mit geeigneten IT-Systemen zur Verfügung zu stellen. IT-Sicherheit ist eine wichtige Voraussetzung für den effizienten Geschäftsablauf innerhalb des BM.I; sie erfordert eine angemessen hohe Verfügbarkeit der Informationssysteme, aktuelle und zuverlässige Daten und einen reibungslosen Informationsfluss. Um dieses Zieles zu erreichen, ist es notwendig, einen IT-Sicherheitsmanagement-Prozess zu etablieren, der die Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Verbindlichkeit und Zuverlässigkeit von Systemen und

Verfahren der Informationstechnik gewährleistet. Die Strategien und Konzepte dieses Prozesses sind laufend auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf in angemessener Form fortzuschreiben und anzupassen.

## Die IT-Sicherheitspolitik des BM.I.

In der ersten Phase des IT-Sicherheitsmanagement-Prozesses wurde ein mit dem A-SIT abgestimmtes Grundsatzdokument IT-Sicherheit – Grundsätze zur IT-Sicherheitspolitik des BM.I" erarbeitet. Es erläutert die Bedeutung von Informationen für das Ressort und bildet den Rahmen für konkrete IT-Sicherheitsrichtlinien und daraus resultierende Maßnahmen. Die IT-Sicherheitspolitik soll insbesondere Verantwortungen regeln; das Bewusstsein für die Notwendigkeit und Einhaltung aller der Informationssicherheit dienenden Vorkehrungen fördern; 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.

## IT-Sicherheitshandbuch

Die Grundlage für die Vorgehensweise bei der Erstellung der IT-Sicherheitspolitik des BM.I ist das österreichische IT-Sicherheitshandbuch. Es bietet auf die österreichischen Rechtsnormen, Standards und Terminologien angepasste Leitlinien und Vorgaben, 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. Das BM.I war treibende Kraft bei der Erstellung des Handbuchs.

Die IT-Sicherheitspolitik des Ressorts als strategisches Grundsatzpapier 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. Für die Umsetzung der IT-Sicherheitspolitik ist die Mitwirkung aller Mitarbeiterinnen und Mitarbeiter des Innenressorts notwendig und vor allem deren Verständnis für die Sinnhaftigkeit und Notwendigkeit der einzelnen Maßnahmen. Um dieses IT-Sicherheitsbewusstsein bei den Mitarbeiterinnen und Mitarbeitern weiter aufzubauen, sowie um den generellen Prozess des ressortweiten IT-Sicherheitsmanagements koordiniert und mit der notwendigen Qualität ablaufen lassen zu können, hat die Ressortleitung einen IT-Sicherheitsbeauftragten (Dipl.-Ing. Robert Gottwald) für das BM.I und alle nachgeordneten Behörden und Dienststellen eingerichtet.

IT-Sicherheitspolitik im Internet: http://www.bmi.gv.at/; im BMI-Intranet: itsich.bmi.intra.gv.at nachzulesen.