



## **IT-SICHERHEIT**

Bei der Kommunikation zwischen Behörden oder zwischen BürgerInnen und Behörden ist es von großer Bedeutung, dass sichere Kommunikation gewährleistet ist, z.B. beim Versenden von sensiblen Daten. IT-Sicherheit als Grundlage für Datensicherheit bildet einen wichtigen Bestandteil des Datenschutzes und gewährleistet etwa die Integrität und Authentizität der Dokumente

### **Hauptpunkte der IT-Sicherheit**

- Vertraulichkeit: (keine Möglichkeit zur unbemerkten und unautorisierten Kenntnisnahme der Daten)
- Integrität: (die Vollständigkeit und Richtigkeit der Daten zu bestätigen sowie Datenmanipulationen zu entdecken)
- Authentizität: (die Echtheit und Glaubwürdigkeit von Objekten zu garantieren)
- Verfügbarkeit: (Verfügbarkeit und Funktionsfähigkeit der Systeme und Dienste sicherzustellen)
- Verbindlichkeit/non-Denial: (die Rechtsgültigkeit von Aktionen zu gewährleisten)
- Privatsphäre, Datenschutz und Datensicherheit: (im Sinne des Datenschutzes unter anderem die Anonymität und die Verhinderung der Profilerstellung über Einzelne sicherzustellen)

### **Drei generelle Sicherheitsstufen sind geplant:**

- üblicher e-Mail-Verkehr über Internet
- Übertragung persönlicher Daten über das Internet mit höheren Sicherheitsanforderungen über gesicherte Zugänge
- Übertragung von Verfahrensdaten mit Hochsicherheitsanspruch

### **Vorgaben und Richtlinien**

Um den verantwortungsvollen Umgang mit persönlichen Daten der BürgerInnen garantieren zu können, wird kontinuierlich an der Schaffung von geeigneten Normen, Richtlinien und Empfehlungen gearbeitet. Verschiedenste themenspezifische Arbeitsgruppen befassen sich mit den unterschiedlichen Aspekten der IT-Sicherheit.

### **Intranet des Bundes**

Ziel ist es, derzeit komplizierte und lokal eingeschränkte Zugänge zum Intranet nunmehr einfach und sicher zu ermöglichen. Zukünftig sollen dann Dienste, die zuvor nur am Dienstort verfügbar waren, in kontrollierter Weise auch dezentral angeboten werden. Zu diesem Zweck wurde der Begriff der Sicherheitsdomäne definiert und darauf aufbauend die einzelnen Zugangsarten kategorisiert. Die dafür notwendigen Charakteristika beziehen sich auf z.B. die Verwendung eines Dienstgerätes, auf Dienste der eigenen oder einer fremden Dienststelle, die eingesetzte Technologie und auch den aktuellen Standort. Parallel zu den Zugangsarten wurden auch Nutzerkategorien abgeleitet, für die schlussendlich unterschiedliche Policies gelten.



## **IT-Sicherheitshandbuch**

Das IT-Sicherheitshandbuch beschreibt grundlegende Sicherheitsaspekte und Sicherheitsmaßnahmen in der Informationstechnologie. Es versteht sich als Sammlung von Leitlinien und Empfehlungen, die entsprechend den spezifischen Anforderungen und Bedürfnissen der anwendenden Organisationseinheiten angepasst werden sollten und stellt somit eine Ergänzung zu den bestehenden Gesetzen, Regelungen und Vorschriften dar. Der erste Teil des Sicherheitshandbuches "IT-Sicherheits-Management" beinhaltet konkrete Anleitungen zur Etablierung eines umfassenden und kontinuierlichen IKT-Sicherheitsprozesses innerhalb einer Organisation. Im zweiten Teil "IT-Sicherheits-Maßnahmen" sind organisatorische, personelle, infrastrukturelle und technische Sicherheitsmaßnahmen für IKT-Systeme beschrieben.

## **Netzwerksicherheit im Bereich e-Government**

Diese Richtlinie befindet sich noch in der Bearbeitungsphase. Ihr Inhalt ist die technische Netzwerksicherheit als Teil der IT-Sicherheit.

## **OECD-Richtlinien für die Sicherheit von Informationssystemen und -netzen**

Die Mitglieder der OECD (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung) haben eine neue Leitlinie entworfen, um auf die zunehmenden Bedrohungen wie Cyber-Terrorismus, Computerviren und Hackangriffe zu reagieren. Die Leitlinien demonstrieren die Verpflichtungen der OECD-Regierungen zu einer stabilen, sicheren und produktiven Entwicklung der Online-Kommunikation.

## **Die Sicherheits- und Verteidigungsdoktrin**

Der Nationalrat hat am 12. Dezember 2001 die neue österreichische Sicherheits- und Verteidigungsdoktrin beschlossen. Inhalt dieser Doktrin ist das Ersuchen an die Bundesregierung, für alle sicherheitspolitisch relevanten Bereiche Teilstrategien auszuarbeiten.

Die Teilstrategie IKT-Sicherheit als Bestandteil der Sicherheits- und Verteidigungsdoktrin wurde termingerecht Anfang Dezember 2002 fertiggestellt und noch im Dezember mit Beschluss des IKT-Boards zur Kenntnis genommen. Derzeit erfolgt die Erarbeitung eines Ministerratsentwurfes für die gesamte Sicherheits- und Verteidigungsdoktrin. Ein Zeitpunkt für die Behandlung im Ministerrat ist auf Grund der derzeitigen politischen Situation zur Zeit nicht vorhersehbar. Die Teilstrategie IKT-Sicherheit wird sofort nach Behandlung im Ministerrat u.a. auf der Homepage des CIO (<http://www.cio.gv.at>) veröffentlicht werden.

## **VPN**

Die grundsätzliche Idee eines VPN (virtual private network) ist es, die Vorteile einer offenen Kommunikationsinfrastruktur ohne Einschränkung der Sicherheit zu nutzen. Ein VPN soll gewährleisten, dass sensible Daten vertrauenswürdig übertragen werden und nur berechnigte Personen an der Kommunikation teilnehmen bzw. auf den Daten definierte Aktionen (wie z.B. Lesen, Ändern, etc.) durchführen dürfen.