Merkblatt IT-Sicherheit

Im Jahr 2005 hat das Land Hessen erstmals eine verbindliche **IT-Sicherheitsleitlinie** in Kraft gesetzt, die in 2009 nochmals überarbeitet wurde. Ziel der IT-Sicherheitsleitlinie ist es, mit Hilfe eines umfassenden IT-Sicherheitsmanagements die Datensicherheit und den Datenschutz zu gewährleisten. Daher sollten Sie dieses Merkblatt sorgfältig durchlesen.

Was bedeutet IT-Sicherheit?

Es gibt mehrere Grundwerte der Informationssicherheit:

Informationssicherheit

Vertraulichkeit	Verfügbarkeit	Integrität	Authentizität
Schutz vertraulicher Informationen vor unbefugter Preisgabe	Informationen zur rechten Zeit am rechten Ort	Unversehrtheit und Korrektheit der Daten Daten sind vollständig und unverändert	Sicherstellung Identität der informations-erzeugenden Person (z.B. durch Anmelde-prozeduren mit Username u. Passwort oder Überprüfung von biometrischen Daten

Diese hochgefassten Begriffe müssen im Detail in vielen Schritten umgesetzt werden. Der Landesbeauftragte für den Datenschutz setzt voraus, das für jedes IT-System, in dem personenbezogene Daten verarbeitet werden oder das hierfür geeignet ist, die für dieses System vom Grundschutzhandbuch empfohlenen Maßnahmen realisiert werden müssen.

Als Institution für die IT-Sicherheit wurde im LLH ein **IT-Sicherheitsbeauftragter** eingesetzt, der verantwortlich ist für die Wahrnehmung aller Belange der IT-Sicherheit innerhalb der Organisation. Zur Realisierung der IT-Sicherheitsmaßnahmen und der Prüfung der Wirksamkeit der Maßnahmen existiert ein IT-Sicherheitsteam. In den letzten Jahren wurden bereits viele Dinge der IT-Sicherheit umgesetzt. Der Übergang zu einem zentralen IT-System (zentrale Benutzerverwaltung, LLH-Desktop und zentrale Datenablage) mit einheitlicher Administration war ein Weg zu mehr IT-Sicherheit.

Bitte verwechseln Sie nicht die Sicherheitsstrategien auf einem häuslichen PC mit denen einer mittelgroßen Behörde, denn die Maßnahmen gehen weit über den Einsatz von Virenschutzprogrammen, replizierter Datenspeicherung und dem Einsatz von Firewall-Systemen hinaus. Für die IT-Sicherheit wird neben der Infrastruktur (Gebäude, Räumlichkeiten, Verkabelung), der IT-Technik (Server, Clients, Betriebssysteme, Netz, Schnittstellen) ebenso die Anwendungen, Organisation von Abläufen, Benutzerverwaltung, Datenhaltung (z.B. Datenbanken, Archive) und auch die Wartung betrachtet.

Die Neufassung der IT-Sicherheitsleitlinie des Landes Hessen in 2009 wird weitere Schritte nach sich ziehen. So müssen alle Fachanwendungen des LLH auf aktuelle Risiken überprüft werden und entsprechend den Standards des Bundesamtes für Informationssicherheit (BSI, IT-Grundschutz) angepasst werden. Dazu werden Sicherheitskonzepte entwickelt, bei denen die Gremien entsprechend den Beteiligungsrechten einbezogen werden. Für alle Verfahren müssen verantwortliche Personen benannt werden, die den Schutzbedarf und die Zugriffsberechtigungen bestimmen. Die erreichten Standards müssen in regelmäßigen Abständen überprüft und gegebenenfalls angepasst werden.

Sicherheitsmaßnahmen sind auch dann anzuwenden, wenn sich daraus Beeinträchtigungen für die IT-Nutzung ergeben. Der monatliche Passwortwechsel ist zwingend nach den Sicherheitsrichtlinien erforderlich, auch wenn für diesen Wechsel von jedem Beschäftigten zusätzliche Zeit benötigt wird. Sollten im Einzelfall Fachanwendungen trotz Sicherheitsvorkehrungen risikobehaftet sein, ist auf den Einsatz einer solchen Fachanwendung zu verzichten.

Hauptziel des IT-Sicherheitsprozesses ist, dass die Beschäftigten des LLH die Informationssicherheit durch verantwortliches Handeln gewährleisten und die Vorschriften einhalten. Im LLH wird auch in zukünftigen Jahren weiter an der IT-Sicherheit gearbeitet, wobei praktisch jeder Bedienstete daran beteiligt sein wird. Eine weitere Sensibilisierung für dieses Thema ist notwendig und wird durch verschiedenste Maßnahmen begleitet.