TOMs für Uni Cloud

Vorwort

Spezifischere Beschreibungen und ergänzende Maßnahmen werden im Sicherheitskonzept der Uni Cloud festgelegt. Das aktuelle Sicherheitskonzept kann auf Anfrage eingesehen werden.

Geltungsbereich für die technischen und organisatorischen Maßnahmen

Die in diesem Dokument beschriebenen technischen und organisatorischen Maßnahmen (TOM) sind gem. Art. 32 DSGVO auf die vom CIT bereitgestellten und verwalteten IT-Systeme aus dem Bereich Uni Cloud verpflichtend anzuwenden. Sie sind ergänzend zu den allgemeinen TOMs des CIT.

Verschlüsselung

- Sämtliche Datenträger in Servern der Uni Cloud sind verschlüsselt.
- Sofern in den Übertragungsprotokollen vorgesehen, werden verschlüsselte Möglichkeiten zur Datenübertragung angeboten.

Vertraulichkeit

Zugangskontrolle

Ein unbefugter Zugang zu IT-Systemen der Uni Cloud ist durch die nachfolgenden Maßnahmen auszuschließen:

- Der administrative Zugang wird nur Administratoren der Uni Cloud gestattet.
- Administratoren müssen sich gegenüber den Systemen authentifizieren.

Zugriffskontrolle

Ein unbefugter Zugriff auf Daten (Lesen, Bearbeiten, Kopieren, Löschen) ist durch folgende Maßnahmen auszuschließen:

- Administrative Zugriffsrechte: Administrative Zugriffsrechte zu Daten auf der Uni Cloud erhalten nur Administratoren der Uni Cloud.
- Zugriffsberechtichtigungen: Nutzer der Uni Cloud haben die Möglichkeit, den Zugriff auf Ihre Daten in der Uni Cloud bezüglich anderer nichtadministrativer Benutzer einzuschränken. Die Berechtigungen bei Freigaben, die von der Uni Cloud über verschiedene Protokolle und Systeme angeboten werden, können anhand von zentral am CIT verwalteten Benutzern und Benutzergruppen vergeben werden.
- Ereignisprotokollierung: Sämtliche Anmeldeereignisse und –versuche an Servern oder Anwendungen werden aufgezeichnet. Sicherheitskritische Änderungen oder Änderungsversuche an Systemdateien auf Servern werden protokolliert.
- Protokollierung: Protokolldateien aller Systeme der Uni Cloud werden zentral gesammelt.

Sicherstellung der Integrität

Weitergabekontrolle

- Datenübertragung: Die Integrität bei der Übertragung von Daten kann, sofern im Protokoll vorgesehen, durch optionale Verschlüsslung oder Signaturen sichergestellt werden.

Datenspeicherung

- Die Integrität von Daten wird auf unterster Ebene durch Prüfsummen gewährleistet.

Verfügbarkeit und Belastbarkeit

Sicherstellung

Die Sicherstellung der Verfügbarkeit als auch der Belastbarkeit der Daten ist durch die nachfolgenden Maßnahmen sichergestellt:

- Ausfallsicherheit: Alle kritischen Systemdienste werden redundant betrieben.
- Datensicherung: Benutzerdaten werden an einem Standort redundant gespeichert, so dass sie gegenüber einzelnen Festplattenausfällen oder Ausfällen einzelner Server gesichert sind.
- Monitoring: Kritische Systeme werden über Monitoring Tools kontinuierlich überwacht.

Wiederherstellung

Die Wiederherstellung der Daten im Fehlerfall ist durch die nachfolgenden Maßnahmen sichergestellt:

- Konsistenzprüfung: Benutzerdaten werden regelmäßig auf deren Integrität anhand von Prüfsummen getestet.
- Redundanzen: Bei erkannten Hardwarefehlern bzw. Integritätsfehlern werden die Redundanzen der Daten an einem Standort automatisch wiederhergestellt.

Wirksamkeitskontrolle

Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen sind sichergestellt durch:

Autoren

Dr. Markus Blank-Burian (CIT, Abteilung 6: Systeme)