TOMs für OpenStack

Vorwort

Diese Maßnahmen beziehen sich ausschließlich auf das OpenStack der Uni Cloud Münster. Spezifischere Beschreibungen und ergänzende Maßnahmen werden im Betriebskonzept vom OpenStack der Uni Cloud Münster festgelegt. Das aktuelle Betriebskonzept 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 der Universität Münster CIT bereitgestellten und verwalteten IT-Systeme aus dem Bereich OpenStack verpflichtend anzuwenden. Sie sind ergänzend zu den allgemeinen TOMs der Universität Münster CIT.

Verschlüsselung

- Sämtliche Datenträger in Servern des OpenStacks sind verschlüsselt.
- Sofern in den Übertragungsprotokollen vorgesehen, werden verschlüsselte Möglichkeiten zur Datenübertragung angeboten.

Vertraulichkeit

Zugangskontrolle

Ein unbefugter Zugang zu IT-Systemen des OpenStacks ist durch die nachfolgenden Maßnahmen auszuschließen:

- Der administrative Zugang wird nur Administratoren des OpenStacks 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 im OpenStack erhalten nur Administratoren des OpenStacks.
- Zugriffsberechtichtigungen: Nutzer des OpenStacks haben die Möglichkeit, den Zugriff auf Ihre Daten im OpenStack bezüglich anderer nichtadministrativer Benutzer einzuschränken. Die Berechtigungen bei Freigaben, die vom OpenStack über verschiedene Protokolle und Systeme angeboten werden, können anhand von zentral an der Universität Münster 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 des OpenStacks 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 nach- folgenden 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 sicher- gestellt:

- 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