Technische und organisatorische Maßnahmen für Sciebo

Technical and organizational measures for University of Münster Sciebo Sync and Share service (in german language)

Vorwort

Diese Maßnahmen beziehen sich ausschließlich auf den Dienst sciebo der Uni Münster, der für alle Hochschulen des Landes NRW angeboten wird.

Geltungsbereich für die technischen und organisatorischen Maßnahmen

Die in diesem Dokument beschriebenen technischen und organisatorischen Maßnahmen (TOM) werden gem. Art. 32 DSGVO auf die vom der Universität Münster CIT bereitgestellten und verwalteten IT-Systeme aus dem Bereich Sciebo Sync and Share angewandt. Sie sind ergänzend zu den allgemeinen TOMs des CIT der Universität Münster.

Verschlüsselung

- Sofern umsetzbar, werden unverschlüsselte Transportwege nicht angeboten.

Vertraulichkeit

Zutrittskontrolle

- Serverräume, Räume für Netz-Infrastruktur und Büroräume sind mit Schließanlagen ausgestattet. Die Vergabe von Zutrittsrechten sowie die Ausgabe der Schlüssel erfolgt ausschließlich nach einem internen Nutzer-Rollen-Konzept und wird dokumentiert
- Die Berechtigung zum Betreten der Serverräume ist auf einen eingeschränkten Personenkreis begrenzt und dokumentiert (RL02 Sicherer IT-Betrieb)

Zugangskontrolle

Ein unbefugter Zugang zu Sciebo wird durch die nachfolgenden Maßnahmen ausgeschlossen:

- Der administrative Zugang wird nur Administratoren von Sciebo gestattet.
- Administratoren müssen sich gegenüber den Systemen authentifizieren.
- Ein administrativer Zugang ist nur aus dem Adminnetz der Abteilung 6 des CIT möglich

Zugriffskontrolle

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

- Administrative Zugriffsrechte: Administrative Zugriffsrechte zu Daten in Sciebo erhalten nur Administratoren
- Die Administratoren verwenden personalisierte Admin-Accounts, die mit MFA abgesichert sind (TOTP über das Webinterface, ssh-keys mit Passwort über die Kommandozeile, Zugriff nur aus abgesichertem Netz, bzw. spezifizierten Jumphosts)
- Zugriffsberechtichtigungen: Standardmäßig können die Nutzenden nur ihr eigenes Datenverzeichnis einsehen. Über Shares in der eingesetzten Software owncloud können anderen Nutzenden Zugriffsrechte gewährt werden
- Ereignisprotokollierung: Sicherheitskritische Änderungen an Systemdateien werden versioniert, protokolliert und deklarativ provisioniert.
- Protokollierung: Protokolldateien aller Server von Sciebo werden zentral gesammelt.
- Brute Force Schutz: Über den mit owncloud gelieferten Schutzmechanismus wird verhindert, dass auf Accounts per Brute Force zugrgriffen werden kann
- 2 Faktor Authentifizierung: Accounts können optional mit einem zweiten Faktor (OTP) gesichert werden
- Sicherheitsupdates: Sicherheitskritische Komponenten wie Apache und php werden bei Bekanntwerden von Sicherheitslücken, mindestens aber monatlich aktualisiert.

Sicherstellung der Integrität

Weitergabekontrolle

- Vor der Weitergabe von Informationen muss stets ihr Schutzbedarf geprüft werden und ob bzw. wie sie weitergegeben werden dürfen.

Datenspeicherung

- Die Integrität von Daten wird auf unterster Ebene durch Prüfsummen gewährleistet.
- Die Daten sind auf RAID-Ebene mit Triple Parity gesichert, d.h. der gleichzeitige Ausfall von drei Festplatten wird ohne Datenverlust verkraftet
- Snapshots, die mindestens 30 Tage aufbewahrt sind, schützen vor ungewolltem Löschen der Daten
- Spiegelung der Daten: Alle Daten werden synchron zwischen zwei Standorten gespiegelt

Verfügbarkeit und Belastbarkeit

Sicherstellung

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

- Ausfallsicherheit: Alle Server des Dateisystems werden redundant betrieben.
- Datensicherung: Benutzerdaten werden an zwei Standorten redundant gespeichert, so dass sie gegenüber einzelnen Festplattenausfällen, Ausfällen einzelner Server oder dem Ausfall eines Serverraums 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.
- Es findet kein Backup auf Band statt

Wirksamkeitskontrolle

Es findet eine regelmäßige Überprüfung, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen statt.

Autoren

- Holger Angenent
- Marcel Wunderlich

Stand

27.4.2024