IT-Sicherheitsmassnahmen ausgewählter ZI-Infrastruktur-Services

Die Zentrale Informatik (ZI) der Universität Zürich lehnt sich bei der Umsetzung ihrer Sicherheitsmassnahmen an die ISO-27001 Norm an. Dazu wurden entsprechende Vorgaben in Weisungen, Reglementen und Merkblättern erstellt. Die Zentrale Informatik ist nicht ISO-27001 zertifiziert.

Sicherheitsrelevante Vorgaben der Zentralen Informatik

Eine Übersicht über die Sicherheitsregeln und Richtlinien findet sich auf folgender Seite: Richtlinien und Sicherheitsregeln | Zentrale Informatik | UZH. Die sicherheitsrelevanten Vorgaben gelten sowohl für die Zentrale Informatik als Service-Anbieter als auch für die Institute als Service-Nutzende.

Die massgeblichen Verweise zu den unten beschriebenen ZI-Services sind im Folgenden aufgeführt.

- Reglement über den Einsatz von Informatikmitteln
  - Reglement über den Einsatz von Informatikmitteln an der Universität Zürich (REIM)
- Netzwerksicherheit:
  - Weisung über die Netzwerksicherheit (WNS)
  - Beilage zum Merkblatt Trustlevels - Zonenkonzept
  - Merkblatt Definition von Trustlevels und Sicherheitsmassnahmen für Netzwerkzonen der UZH
- Logfile Policy:
  - Weisung für die Protokollierungen von Systemvorgängen (Logfile Policy)
- Betrieb von Systemen:
  - Weisung für den Betrieb von Systemen (WBS)
- Applikationssicherheit:
  - Merkblatt Anforderung an Webapplikation für Applikations- und IT-Verantwortliche

Shared Responsibility Prinzip

Die Zentrale Informatik stellt ihre Services gemäss dem Shared Responsibility Prinzip bereit. Sicherheits- und Betriebsverantwortungen werden zwischen der Zentralen Informatik als Service-Anbieter und dem Institut als Service-Nutzenden aufgeteilt. So wird Klarheit geschaffen, wer für welche Aspekte der IT-Sicherheit und des Betriebs zuständig ist. Eine Beschreibung der Verantwortlichkeiten findet sich in der folgenden Tabelle.

Beschreibung der Verantwortlichkeiten und Sicherheitsmassnahmen ausgewählter Services

Die unten aufgeführten IT-Sicherheitsmassnahmen gelten ausschliesslich für IT-Systeme der Datacenter-Zone 1–4 der ZI. Für die Klärung der Umsetzung der IT-Sicherheitsvorgaben in Umgebungen wie Science IT (S3IT),

NUZ, der Institutszone sowie für «Housing VM's» ist der jeweils zuständige IT-Systemverantwortliche zu kontaktieren.

Service	Verantwortlichkeit ZI	Verantwortlichkeit Service-Nutzender	Sicherheitsmassnahmen ZI
Server Housing - Physical: Instituts-Zone	— Netzwerk-seitige Sicherheit der Instituts-Zone	Für die IT–Sicherheit und den Betrieb der Server ist der Service-Nutzende verantwortlich. Dies betrifft: — Operating System (OS) — Middleware — Applikation inkl. Zugriffssteuerung der Applikation — Netzwerk: Mikrosegmentierung (z.B. lokale System-Firewall)	Umsetzung der Netzwerk-Standardsicherheit: — Firewalls: Konfiguration gemäss Anforderung des Services-Nutzenden — Zugriffskontrollen — Verschlüsselung: wenn verlangt
Managed Virtual Server (und HW-Server) Linux	— Netzwerk — OS — Middleware, die von der ZI zur Verfügung gestellt wird	— Netzwerk: Mikrosegmentierung über lokale Firewall wo notwendig — Applikation inkl. Zugriffssteuerung der Applikation — Middleware, die vom Service-Nutzenden zur Verfügung gestellt wird	— Netzwerk: komplett segmentiertes Netzwerk nach Trustlevel (siehe Vorgaben Netzwerksicherheit) — Zugriffssteuerung: Aktive Zugriffssteuerung durch Basisdienste der ZI (OS-Administration nur durch ZI, externe Zugriffe auf Applikation für Maintenance nur per MFA und Jumphost) — Server sind gehärtet (CIS Hardening) — Server haben keine Administrationsrechte für nicht ZI Sys-Admins, also keine Root Rechte. — Erreichbarkeit der Server für den Unterhalt nur über spezielle Admin-Client Zone (Zugriffe werden kontrolliert und gemonitort) mit zusätzlichem MFA. — Die 4 Datacenter Zonen der ZI werden durch das Security Operation Center der IT-Sicherheitsstelle überwacht. Zusätzlich gibt es jeweils ein operatives Monitoring durch die Fachabteilungen der ZI. — Die Server der Datacenterzonen 1-4 sind in einem Backupservice eingebunden.

Service	Verantwortlichkeit ZI	Verantwortlichkeit Service-Nutzender	Sicherheitsmassnahmen ZI
Managed Virtual Server (und HW-Server) Windows	— Netzwerk — OS — Middleware, die von der ZI zur Verfügung gestellt wird	— Netzwerk: entsprechende Massnahmen müssen durch das Institut in der Windows Firewall erfolgen, Mikrosegmentierung — Applikation inkl. Zugriffssteuerung der Applikation — Middleware, die vom Service-Nutzenden zur Verfügung gestellt wird	— Netzwerk: entsprechende Massnahmen müssen durch das Institut in der Windows Firewall erfolgen — Zugriffssteuerung: Aktive Zugriffssteuerung durch entsprechende Gruppen im Active Directory für Administration und RDS-Users. IT-V haben via OU-Administratoren-Konti Zugriff auf alle VM — Server sind gehärtet (CIS Hardening) — Erreichbarkeit der Server für den Unterhalt (vSphere Client) nur über spezielle Admin-Client Zone (Zugriffe werden kontrolliert und gemonitort) mit zusätzlichem MFA. — Basis-Monitoring der Systeme mit ZI-interner Monitoring Lösung während Büro-Zeiten — Backup der VM erfolgt täglich mit Veeam Backup — Regelmässig automatisiertes Patching der Systeme mit Microsoft Hotfixes bzw. Aktualisierung der zentral angebotenen Applikationen basierend auf dem definierten Wartungsfenster
ZI Container Services	— Netzwerk — OS — Middleware, die von der ZI zur Verfügung gestellt wird	— Applikation (Deployment) inkl. Zugriffssteuerung der Applikation — Middleware, die vom Service-Nutzenden zur Verfügung gestellt wird — Einhaltung der Compliance-Policy für Container	— Aktive Zugriffssteuerung über die Basisdienste der ZI: — Zugriff auf Management-Tools für Administratoren ausschliesslich via MFA und VPN — Zugriff auf Management-Tools für Nutzende ausschliesslich via MFA — Nutzende können Mutationen ausschliesslich in ihren zugewiesenen Namespaces durchführen — Globale Administrationsrechte sind ausschliesslich ZI-Systemadministratoren sowie definierten Personen des externen Partners vorbehalten — Applikationen (Deployments) sind ausschliesslich über gemanagte

Service	Verantwortlichkeit ZI	Verantwortlichkeit Service-Nutzender	Sicherheitsmassnahmen ZI
			und überwachte Loadbalancer-Gateways der Cluster erreichbar
Datenbank-service Micro-soft SQL	— baut auf dem Service «Managed Virtual Server» auf — Datenbank	Zugriffssteuerung der Applikation, die auf die Datenbank zugreift	— Die Datenbankserver stehen in einer separaten Datacenter Netzwerkzone (DC-Zone 3) mit erhöhtem Trustlevel. — Applikationen, welche einen Zugriff auf eine Datenbank benötigen stehen in der DC-Zone 1 oder 2 und werden somit auf einem separaten Server entkoppelt von einer DB betrieben, dadurch gibt es keine direkte, durchgehende Verbindung von der Applikation zu einer DB (Verhinderung Zugriffe auf Daten bei Kompromittierung des Applikationsservers).
Backup - virtuelle & physische Hosts	— baut auf dem Service «Managed Virtual Server» auf	-	Dauer für das Einspielen eines Backups: RTO (Recovery Time Objective) — Self-Service: Instant VM recovery innerhalb von Minuten (ca. 15 – 30 Minuten) — Self-Service: Storage Recovery – kommt auf die Datenmenge an, ca. 1.5 TB/Stunde innerhalb der ersten 30 Tage. — Via TopDesk Ticket: Storage Recovery – von Tape ca. 800GB/Stunde (Für den Fall, dass Recovery von 30-90 Tage benötigt wird). Reaktionszeit auf Topdesk Tickets: ca. 24h RPO (Recovery Point Objective) — Wir sichern täglich, daher gibt es mindestens einen RPO innerhalb 24h.
Campus - LAN (Wired), Campus - WLAN	Netzwerk	-	Umsetzung gemäss den Vorgaben zur Netzwerksicherheit

Regelung der Zugriffssteuerung für Server und Datenbanken der Zentralen Informatik

Die konkreten Regeln und Mechanismen, welche festlegen, wer zu welchem Zeitpunkt und in welcher Form Zugriff auf Ressourcen erhält (z. B. Rollen, Berechtigungen, Firewall-Regeln oder

Authentifizierungsverfahren), werden im Rahmen des Berechtigungs- und Zugriffskonzepts durch die Fachabteilungen der Institute / ZDU und oder Information Owner (verantwortlich für die Datenklassifizierung) gemeinsam mit der ZI definiert.
Die Fachabteilungen sowie die jeweiligen Information Owner sind für die Festlegung der erforderlichen Zugriffsrechte verantwortlich und erstellen ein Role Based Access Konzept. Die ZI stellt die technischen Zugriffsmöglichkeiten sowie die notwendigen Sicherheitsmechanismen bereit. Die konkrete Nutzung der bereitgestellten Zugriffsoptionen wird durch die jeweilige Fachabteilung und oder Information Owner festgelegt und verantwortet.

Weitere Sicherheitsmassnahmen

Überwachung durch Security Operation Center der IT- Sicherheitsstelle
Das Security Operation Center überwacht das Datacenter Zone 1-4 vollständig sowie das Netzwerk der UZH an spezifischen Übergängen. Für die Überwachung der Instituts-Zone sind die Institute selbst verantwortlich.

Audits/Assessments
Folgende Audits wurden in den letzten Jahren durchgeführt:
— Datacenter Assessment der Zonen 1-4 des ZI-Datacenters
— Durchführen von Penetrationtests für Applikationen (laufend seit 2019)
— Red-Teaming zur Überprüfung der Resilienz des Datacenters der Zonen 1-4 der ZI (2024 -2025)
— Purple-Teaming zur Überprüfung der Wirksamkeit des SOC innerhalb der IT – Sicherheitsstelle (2025)

Vulnerability Management
Die IT–Sicherheitsstelle überprüft die DC-Zonen 1-4 alle 3 Monate auf Schwachstellen. Zudem lässt die IT-Sicherheitsstelle alle Domänen per externem Vulnerability Scan laufend überprüfen. Schwachstellenreporte werden wöchentlich ausgewertet und die Befunde an die entsprechenden verantwortlichen Systembetreiber adressiert. Für die Überwachung der Instituts-Zone sind die Institute selbst verantwortlich.

Physische Sicherheit des Datacenters der ZI
Der Zutritt zu den Datacentern der Zentralen Informatik der UZH unterliegt strengen Sicherheitsmassnahmen, die von der ZI verwaltet werden. Zugänge sind durch Überwachungssysteme (Kameras) und Protokollierungen (Logs) gesichert. Server müssen spezifische Vorgaben erfüllen, um dort untergebracht zu werden.
— **Zutrittskontrolle**: Die Hoheit über die Datacenter-Zugänge liegt bei der Zentralen Informatik.
— **Netzwerksicherheit**: Netzwerkkomponenten auf dem UZH-Campus müssen in abschliessbaren Räumen oder Schränken platziert sein.
— **Sicherheitsmassnahmen**: Es kommen Überwachungssysteme wie Kameras und Zugangslogs zum Einsatz.
— **Regeln für Server in Verteilerräumen**: Bei Unterbringung im Datacenter Irchel gelten strenge Auflagen: Keine Lagerung von Material, Temperaturüberwachung, und eigene Racks für Server.