Sicherheitsprofil: Rechenzentren & Prozesse

Dieses Dokument bietet einen Überblick über das ganzheitliche Sicherheitskonzept von HashWerk (hashwerk.eu). Unser "Defense-in-Depth"-Ansatz schützt die uns anvertraute Hardware unserer Kunden durch mehrstufige, ineinandergreifende Sicherheitsmaßnahmen auf physischer, technischer und prozessualer Ebene.

Sicherheitsmaßnahmen im Überblick

Unsere Standorte in der **Türkei** (energieoptimiert) und **Skandinavien** (Wasserkraft, natürliche Kühlung) erfüllen durchgehend die hier beschriebenen hohen Sicherheitsstandards.

Sicherheitsebene	Implementierte Maßnahmen
1. Physische Sicherheit	• **Perimeter-Sicherung:** Geländeumzäunung, alarmgesicherte Zugänge und Videoüberwachung des Außenbereichs. • **Mehrstufiges Zugangssystem:** Autorisierung über Mehr-Faktor-Authentifizierung (Chipkarte, PIN, optional Biometrie). • **24/7 Videoüberwachung:** Lückenlose, hochauflösende Aufzeichnung aller sicherheitsrelevanten Bereiche, insbesondere der Serverräume. • **Besucher-Management:** Zugang für Dritte ausschließlich mit Voranmeldung, Identitätsprüfung und in Begleitung von

	autorisiertem Personal.
2. Technische Sicherheit	• **Redundante Stromversorgung:** Mehrfache Netzeinspeisung, N+1 USV-Anlagen und Notstromaggregate (Diesel) mit Kraftstoffvorrat für min. 48 Stunden autonomen Betrieb. • **Redundante Netzwerkverbindungen:** Anbindung über mehrere Carrier zur Gewährleistung der Konnektivität. • **DDoS-Schutz:** Automatisierte Erkennung und Filterung von Distributed-Denial-of-Service-Angriffen auf Netzwerkebene. • **Klimatisierung & Brandschutz:** Redundante Kühlsysteme, permanente Überwachung von Temperatur und Luftfeuchtigkeit, Brandfrüherkennung und automatische Löschsysteme (Gas).
3. Prozessuale Sicherheit	• **24/7 Monitoring (NOC):** Permanente Überwachung aller Systeme durch unser Network Operation Center. • **Definierte Eskalationspläne:** Klare Handlungsanweisungen für Störungen (Temperatur, Strom, Netzwerk). • **Regelmäßige Hardware-Checks:** Präventive Wartung der Infrastruktur und der Kundenhardware (Sichtprüfung von Filtern, Lüftern, Kabelverbindungen). • **Wartungsprotokolle:** Lückenlose Dokumentation aller durchgeführten Arbeiten.
4. Personelle Sicherheit	• **Personalüberprüfung:** Sicherheitsüberprüfung und Verpflichtung zur Vertraulichkeit (NDA) für alle Mitarbeiter mit Zugang zu sensiblen Bereichen.

	• **Schulungen:** Regelmäßige Schulungen des Personals zu Sicherheitsprotokollen und Notfallverfahren. • **Rollenbasiertes Zugriffskonzept (RBAC):** Mitarbeiter erhalten nur die Zugriffsrechte, die für ihre jeweilige Aufgabe zwingend erforderlich sind.
5. Compliance & Datenschutz	• **DSGVO-Konformität:** Strenge Verarbeitung von Kundendaten nach EU-DSGVO. Es werden ausschließlich für die Vertragserfüllung notwendige Daten erhoben. • **Zero-Trust bei Kunden-Assets:** Wir speichern oder verwalten zu keinem Zeitpunkt private Wallet-Keys. Auszahlungen gehen direkt vom Mining-Pool an die Kundenwallet. • **Prozessorientierung nach ISO/IEC 27001:** Unsere internen Prozesse für das Informationssicherheits-Management (ISMS) orientieren sich an den international anerkannten Standards der ISO 27001.

6. Transparenz und Kundenkontrolle

Sicherheit bedeutet für uns auch Transparenz. Unsere Kunden profitieren von:

- **Monitoring-Zugriff:** Auf Wunsch gewähren wir einen Einblick in das Monitoring-Dashboard zur Überwachung der eigenen Hardware-Performance.
- **Regelmäßigen Reports:** Auf Anfrage stellen wir Berichte zur Standort-Performance und zur Uptime der Hardware bereit.
- **Proaktiver Kommunikation:** Alle geplanten Wartungsfenster werden frühzeitig und transparent kommuniziert.