Systembeschreibung gemäß BSI C5

Steffen Ritter - 2026-07-14 - Fragen zum Produkt

Über die Bare.ID GmbH

Die Bare.ID GmbH, mit Sitz in 65185 Wiesbaden ist ein deutsches Unternehmen das mit der Lösung "Bare.ID" eine Identitäts- und Zugriffsmanagement-Lösung (IAM) mit Single Sign-On (SSO) und Mehrfaktor-Authentifzierungs-Funktionalitäten (MFA) auf Basis des OpenSource IAM-Frameworks entwickelt und sowohl als "Self-Hosted"-Lizenz bereitstellt wie auch als SaaS (Software-As-A-Service)-Plattform Kunden zur Verfügung stellt.
Für die Bare.ID GmbH ist digitale Souveränität in höchstem Maße wichtig: Jegliche Standorte der Bare.ID GmbH, Ihre Eigentümerstruktur sowie Dienstleister in Berührung mit Kundendaten sind in und aus Deutschland, wodurch der Dienst zweifelsfrei deutscher Gerichtsbarkeit unterliegt.

Die Bare.ID GmbH als Betreiber des Dienstes ist ohne Ausnahmen im Geltungsbereich oder eingeschränktem Scope nach ISO27001:2022 von der DaKKS akkreditierten Prüfstelle des TÜV Rheinland zertifiziert. Nicht zertifiziert, aber angelehnt an die entsprechenden Standards sind das Busines Continuity Manamgent nach BSI 200-4 und Qualitätsmanagement nach ISO 9001. Unser externer Datenschutzbeauftragter überprüft jährlich die Vorgaben nach dem Datenschutz und hat der Bare.ID GmbH wiederholt Konformität mit der DSGVO bescheinigt.

Die SaaS-Plattform

Die Bare.ID SaaS-Lösung ermöglicht Kunden die von Bare.ID entwickelte Software-Lösung im Rahmen des IT-Sourcings ohne eigene Betriebs- und Rechenzentrumskapazitäten zur Absicherung von Login und Identifikationsprozessen einzusetzen. Die Dienstleistungen schließen Nebenleistungen wie Managed-Cloud-Services mit ein.

In der Bare.ID SaaS-Plattform stellt die Bare.ID GmbH auf Basis mehrerer geo-redundanter Kubernetes-Cluster jedem Kunden einen für diesen Kunden dedizierten Stack an Storage, Datenbank-, Anwendungs-Workloads bereit, die durch entsprechende Policies im Kubernetes und das Service-Mesh von einander separiert sind. Die Kubernetes Cluster, die gemeinsam ein Region Pair bilden sind gemäß der BSI Vorgaben an Hochverfügbarkeit georedundant. Vor allem eingehenden Netzwerkverkehr ist die Myra-DDoS-Protection als Schutzlayer und TLS-Offloading eingesetzt. Der Kunde kann Bare.ID vollständig einsetzen, ohne von Bare.ID bereitgestellte Software-Komponenten in seinem Verantwortungsbereich installieren zu müssen - Bare.ID funktioniert vollständig Browserbasiert.

Bare.ID setzt zur Bereitstellung seiner Leistungen ausschließlich auf Server innerhalb der Bundesrepublik Deutschland. Im speziellen sind dies der Rechenzentren der SysEleven GmbH in Berlin, Hamburg, Düsseldorf und Frankfurt sowie der Hetzner GmbH in Falkenstein und Nürnberg, die jeweils für sich mit 99,5% Verfügbarkeit Bare.ID zur Verfügung gestellt werden. Diese Dienstleister sind vollständig für die Physikalische Sicherheit Ihrer Rechenzentren sowie die Inbetriebnahme der jeweiligen Server und Netzwerkassets verantwortlich.
Durch georedundante und resiliente Setups kann Bare.ID eine Verfügbarkeitsgarantie von 99,9% im monatsmittel vertraglich garantieren (SaaS-AGB Punkt II.2.4) was der Verfügbarkeitsklasse VK1 im Sinne der EVB IT Cloud entspricht.

Im Rahmen der "Managed-Cloud-Services" sind Support, Fehler und Störungsbeseitigung integrierter Teil des SaaS-Betriebes. In diesem Rahmen existieren für Bare.ID vier definierte Fehlerklassen, wobei die ersten drei mit den EVB IT Cloud Störungsklassen korrespondieren: Abhängig von der jeweiligen Fehlerklasse garantiert Bare.ID Reaktionszeiten bei Störungsmeldungen und bietet - je nach Vertraglicher Ausprägung - eine 24/7 erreichbare Notfallhotline. Bei Nichteinhaltung stehen dem Kunden - je nach Schwere - Erstattungs- und Sonderkündigungsrechte zu. Ein Anspruch auf eine definierte Wiederherstellungszeit ist nicht gegeben. Im Rahmen des regulären, georedundanten Betriebes sichert Bare.ID RTO und RPO zu, verzichtet aber auf

Zusicherungen bezüglich eines Notbetriebes, da dieser durch die standardmäßige Geo-Redundanz nicht zum tragen kommen sollte.

Die Daten des Kunden sind zu jeder Zeit Transportverschlüsselt (TLS >1.2) - sowohl im Cluster zwischen den Diensten, zwischen den Kubernetes North/South Gateway und der Myra-Protection und vom Nutzer zur Myra-Application. Datenbanken und deren Backups sind AES 256 "at Rest" mit Kunden eigenen, aber von Bare.ID verwalteten, Schlüsseln verschlüsselt.

Das System speichert Audit- und Event-Logs für 90 Tage und stellt diese sowohl dem Kunden als auch dem Betriebsteam zur Verfügung. Verschiedene Integrationen erlauben die nahtlose Anbindung in Kunden-SIEM-Systeme und werden bei Bare.ID für kontinuierliches Monitoring und Alerting in Form anonymer Metriken überwacht. Bare.ID setzt dabei auf einen öffentlich verfügbaren und marktüblichen selbstbetriebenen Observability-Stack mit dem auch das allgemeine Logging, Monitoring und Incident-Management abgebildet wird.

Dem Kunden wird Zugang zur einer Administrationsoberfläche gewährt, in der er die Leistungen der Bare.ID SaaS-Plattform frei konfigurieren kann. Bare.ID schützt diese Zugänge durch enstprechende Passwort-Policies, Mehrfaktorauthentifizierung und ein striktes Rollenkonzept sowie Freigabe-Workflows und rät dem Kunden diese Zugänge nach dem Least-Privilege Prinzip zu vergeben. Innerhalb der Security Lösung selbst, ist der Kunde frei wie er diese konfiguriert. Ein "Security Score" weißt den Kunden dabei auf nachteilige Konfigurationen sowie Abweichungen von BSI Vorgaben und Best Practices hin. Die sichere Konfiguration sowie die funktionale Integration der durch Bare.ID bereitgestellten Leistungen bleibt jedoch in der Verantwortung des Kunden.

Der Kunde ist vertraglich dazu verpflichtet die von Bare.ID bereitgestellte Lösung nur gesetzeskonform einzusetzen. Bare.ID wird dem Kunden - im Rahmen des rechtlich Möglichen - einbinden, wenn Behörden Ermittlungen zu Gegenteiligem anstellen, gibt aber im Rahmen seiner gesetzlichen Verpflichtungen bei Bare.ID gespeicherte Daten an berechtigte Behörden heraus.

Aus der Art & Natur der Bare.ID SaaS-Lösung sowie der vorab skizzierten Architektur ergeben sich, das die BSI C5 Kriterien AM-03, AM-04, OPS24, CRY-03, PSS-03, PSS-10, PSS-11 sowie PSS-12 nicht anwendbar sind.