heylogin

Compliance
Whitepaper

der **heylogin GmbH**, Sophienstraße 40, 38118 Braunschweig
für das Produkt heylogin

Stand: 18. November 2021
Version: 1.0

Inhalt

1 | Vertragsvereinbarungen

1.1 Verfügbarkeit

Die heylogin GmbH gewährleistet eine Verfügbarkeit von 99,9% im Jahresmittel. Diese Verfügbarkeit können wir durch unseren Hostinganbieter Hetzner und unsere Architektur sicherstellen.

1.2 Kapazität

heylogin hat keine Limitierungen für die Menge der gespeicherten Logins und Teams. Wir reservieren mindestens 500MB Speicherplatz pro Organisation.

1.3 Kündigung

Abhängig von der Vertragslaufzeit kann zum nächsten Monat oder jährlich gekündigt werden. Nach dem Ende der Vertragslaufzeit sind in Teams gespeicherte Logins für mindestens 30 Tage exportierbar. Alle Team-Funktionen werden nach Ende der Vertragslaufzeit deaktiviert. Es können keine Teams mehr erstellt, bearbeitet oder gelöscht werden. Weiterhin können Logins in Teams nicht mehr benutzt, erstellt und bearbeitet werden. Alle Logindaten sind jederzeit löschbar.

2 | Betrieb

2.1 Server-Standorte

Die heylogin Produktivumgebung befindet sich in Nürnberg, der Standby-Server in Falkenstein. Backups werden separat in Frankfurt gespeichert. Alle verwendeten Rechenzentren sind ISO-27001-zertifiziert (Hetzner-Zertifizierung).

Abbildung 1: ISO 27001-zertifiziertes Informationssicherheits-Management-system des Rechenzentrums

2.2 Ausfallsicherheit

Die Architektur von heylogin erlaubt es uns innerhalb kurzer Zeit eine Ersatzinstanz unserer Produktivumgebung zu starten. Sollte das verwendete Rechenzentrum unseres Hostinganbieters nicht mehr verfügbar sein, gibt es einen Standby-Server, welcher innerhalb einer Wiederanlaufzeit von maximal 30 Minuten zu einer funktionsfähigen Produktivumgebung umfunktioniert werden kann. Hierbei tritt kein Datenlust auf.

Von der serverseitigen Datenbank werden automatisiert stündlich verschlüsselte Backups erstellt. Diese Datenbank wird weiterhin aktiv zu dem vorher genannten Standby-Server in einem anderem Rechenzentrum repliziert. Mit diesem Backup sichern wir uns gegen einen Komplettausfall unseres Hostinganbieters ab. Innerhalb einer Wiederherstellungszeit von maximal 60 Minuten können wir ein neues Produktivsystem bei einem alternativen Hostinganbieter hochfahren. Die heylogin-Clientanwendungen werden in diesen Fall Logindaten, die noch lokal vorhanden sind, wieder mit dem Server abgleichen, sodass die Wahrscheinlichkeit eines Datenverlustes gering ist. Im schlechtesten Fall kann es zu einem Datenverlust von Änderungen kommen, die seit dem letzten stündlichen Backup passiert sind.

2.3 Überwachung

Die heylogin Produktivumgebung wird von einem Monitoringsystem minütlich überwacht. Bei Ausfällen und Anomalien werden Benachrichtigungen verschickt und diese protokolliert.

2.4 Reaktion bei Sicherheitsvorfällen

Alle administrativen Login-Vorgänge auf die Produktivumgebung und den Cold-Standy-Server werden protokolliert und müssen begründet werden. Es ist immer ein*e Mitarbeiter*in in Bereitschaft, um bei Anomalien einzugreifen.

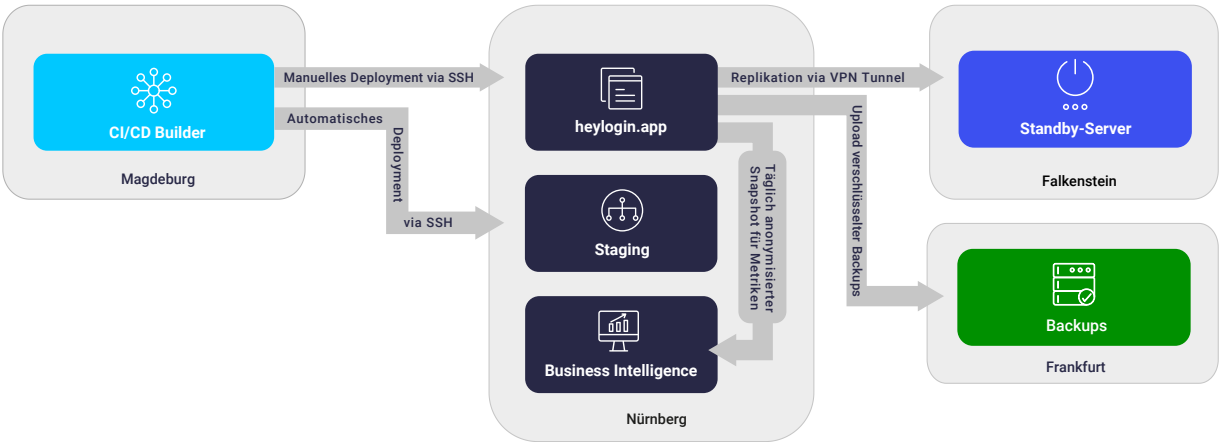


Abbildung 2: Entwicklungsumgebung mit Continuous Deployment (CI), Produktivumgebung und Backup-Systeme sind logisch und physisch voneinander getrennt.

3 | Kryptografie

3.1 Transportverschlüsselung

Die Produktivumgebung nutzt für alle Verbindungen eine Transportverschlüsselung nach aktuellen Standards (TLS 1.3 oder 1.2). Die Nutzung wird durch HSTS erzwungen.

3.2 Verschlüsselung der Server-Backups

Server-Backups werden ausschließlich verschlüsselt gespeichert. Für die symmetrische Verschlüsselung wird ChCha20 und für die Integritätssicherung Poly1305 genutzt.

3.3 Ende-zu-Ende-Verschlüsselung

Die Vertraulichkeit der gespeicherten Daten wird mit einer Ende-zu-Ende-Verschlüsselung sichergestellt. Als symmetrischen Algorithmus wird XSalsa20 eingesetzt. Die Integrität der gespeicherten Daten ist durch Poly1305 sichergestellt und damit gegen Veränderung geschützt. Als asymmetrische Verschlüsselung wird Curve25519 genutzt. heylogin nutzt das in der Smartphone-Hardware eingebettete Secure Element für kryptografische Operationen.

3.4 Ende-zu-Ende-Authentisierung

Alle verbundenen Geräte des Nutzers werden "out-of-band" authentisiert. Dies geschieht normalerweise durch das Scannen eines QR Codes, der einen Diffie-Hellman-Schlüsselaustausch initiiert. Als Alternative für Geräte ohne Kamera kommt ein Hash-Commitment-Verfahren mit Short Authentication String zum Einsatz.

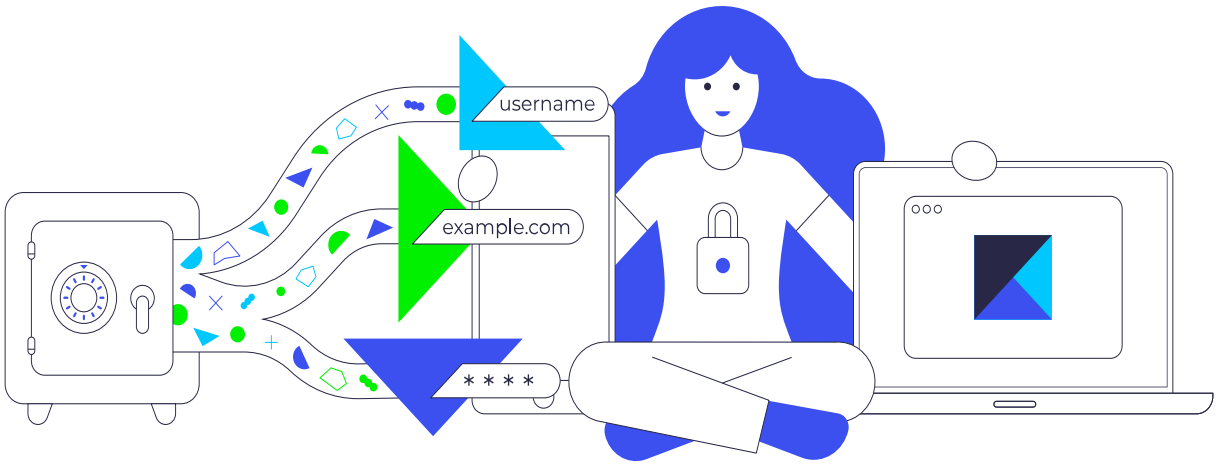


Abbildung 3: Nur das Smartphone des Nutzers kann die Logins entschlüsseln und weitergeben. Ende-zu-Ende-Verschlüsselung & Authentisierung zwischen Smartphone und Browser sorgen dafür, dass keine dritte Instanz Logins mitlesen kann.

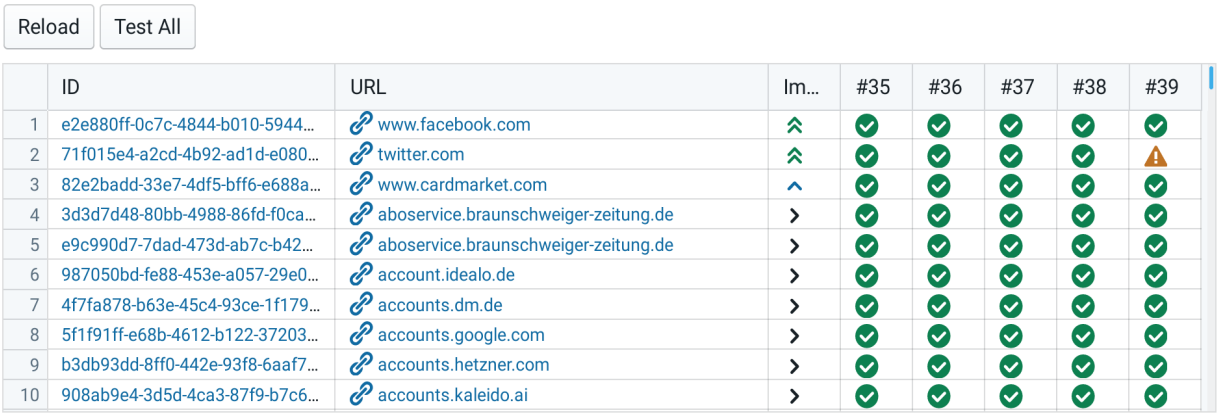
4 | Softwareentwicklung

4.1 Qualitätssicherung

heylogin wird durch eine umfassende Testsuite abgesichert, die automatisiert jede Code-Änderung auf Richtigkeit und Kompatibilität prüft. Wir überprüfen auch automatisiert die Kompatibilität unserer Serveranwendung mit älteren Versionen unserer Clientanwendungen.

Neue Features werden zuerst in internen Review-Apps getestet, bevor diese in die Produktivumgebung integriert werden. Zusätzlich gibt es einen ausgewählten Kreis an Nutzer*innen welche immer die aktuellste Entwicklungsversion der Mobile-App zusammen mit der Produktivumgebung nutzen, um so Fehler möglichst früh entdecken zu können.

Die Kompatibilität der Browser-Extension mit Webseiten wird fortlaufend automatisiert getestet. Wird eine fehlerhafte Webseite gemeldet wird der Algorithmus daraufhin angepasst und diese Webseite in die Testsuite aufgenommen.



	ID	URL	Im...	#35	#36	#37	#38	#39
1	e2e880ff-0c7c-4844-b010-5944...	www.facebook.com						
2	71f015e4-a2cd-4b92-ad1d-e080...	twitter.com						
3	82e2badd-33e7-4df5-bff6-e688a...	www.cardmarket.com						
4	3d3d7d48-80bb-4988-86fd-f0ca...	aboservice.braunschweiger-zeitung.de						
5	e9c990d7-7dad-473d-ab7c-b42...	aboservice.braunschweiger-zeitung.de						
6	987050bd-fe88-453e-a057-29e0...	account.idealo.de						
7	4f7fa878-b63e-45c4-93ce-1f179...	accounts.dm.de						
8	5f1f91ff-e68b-4612-b122-37203...	accounts.google.com						
9	b3db93dd-8ff0-442e-93f8-6aaf7...	accounts.hetzner.com						
10	908ab9e4-3d5d-4ca3-87f9-b7c6...	accounts.kaleido.ai						

Abbildung 4: Automatisierte Kompatibilitätstests für die Browser-Extension

4.2 Fehlerbehandlung

Beim Auftreten eines Applikationsfehlers in einer heylogin-Komponente (Android, iOS, Web, Extension) wird eine Meldung an ein Fehler-Tracking-System gesendet. Diese enthält notwendige Informationen zur Fehlerdiagnose und eine pseudonymisierte Identifikationsnummer, aber niemals inhaltliche Daten.

Basierend auf der Schwere des Fehlers werden Maßnahmen zur Verhinderung weiterer Fehler ergriffen bzw. Änderungen zur Mitigation entwickelt.

4.3 Dokumentation

Die Architektur von heylogin ist im firmeninternen Wiki dokumentiert und für alle Mitarbeiter*innen einsehbar. Wir arbeiten an einem Whitepaper welches unsere technische Architektur in Zukunft detaillierter öffentlich darlegt.

5 | Nachhaltigkeit

5.1 Nachhaltiger Umgang mit Ressourcen

Die heylogin GmbH legt großen Wert auf Nachhaltigkeit. Unser Hostinganbieter Hetzner betreibt seine Rechenzentren zu 100% mit Strom aus regenerativen Quellen. Abgeschriebene Laptops werden an Hey Alter! gespendet und somit von Schüler*innen weitergenutzt.