heylogin

Compliance

Whitepaper

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

Stand: 8. Juli 2022
Version: 1.7

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-Managementsystem 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 lo-

kal 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 Standy-Server werden protokolliert und müssen begründet werden. Es ist immer ein*e Mitarbeiter*in in Bereitschaft, um bei Anomalien einzugreifen.

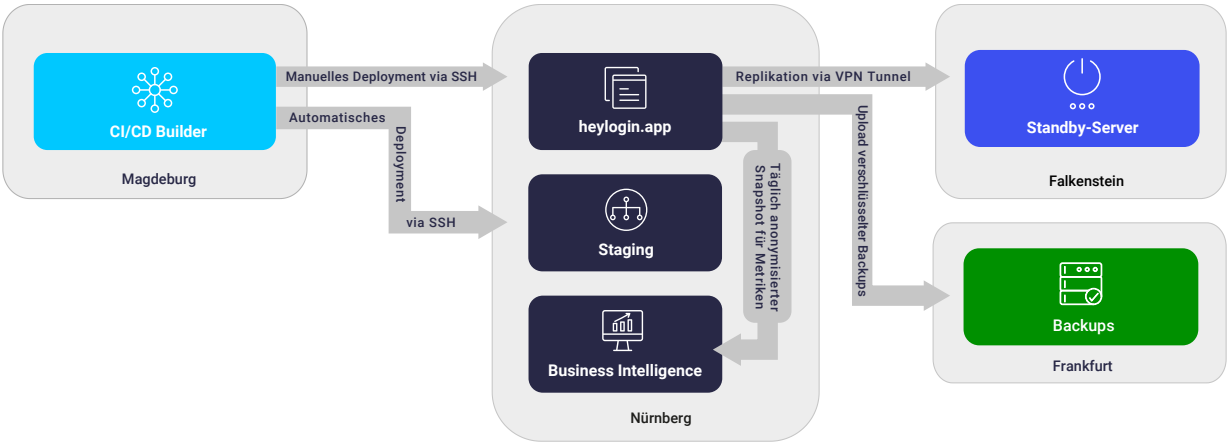

Abbildung 2: Entwicklungsumgebung mit Continuous Deployment (CI), Produktivumgebung und Backup-Systeme sind logisch und physisch voneinander getrennt.

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 ChaCha20 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.

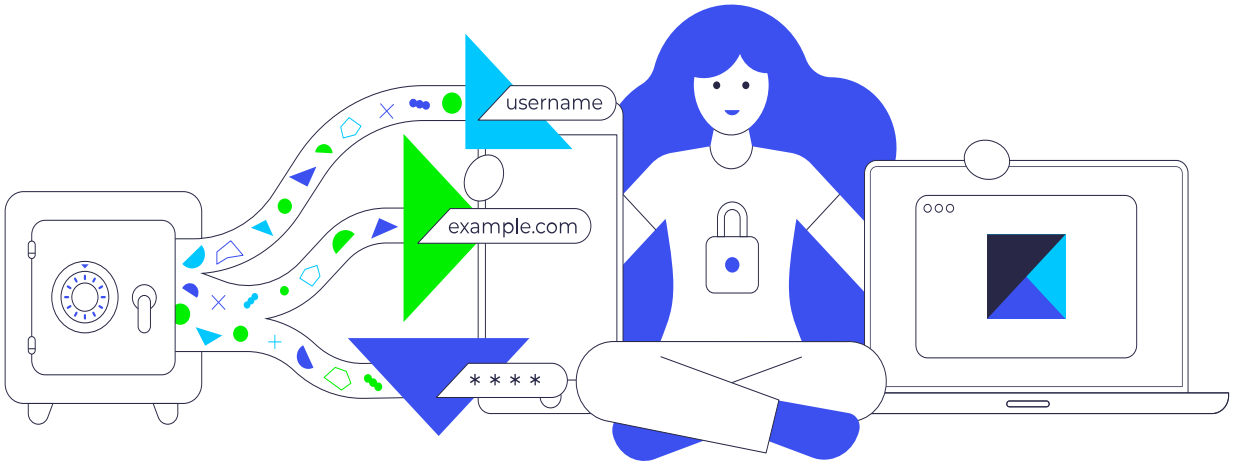

Abbildung 3: Nur das Smartphone des Nutzers kann die Logins entschlüsseln und weitergeben. Ende-zu-Ende-Verschlüsselung & Authentisierung zwischen Smartphone und Browser sorgen dafür, dass keine dritte Instanz Logins mitlesen kann.

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.

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. Details zu heylogins Sicherheitsarchitektur werden in unserem Security Whitepaper dargestellt.

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.

6 | Gesetze, Standards, Zertifizierungen

6.1 Vorwort

Die heylogin GmbH und das Produkt heylogin nutzen moderne Sicherheitsstandards und erfüllen die gesetzlichen Anforderungen der Datenschutz-Grundverordnung (DSGVO). Gleichzeitig kann der Einsatz von heylogin Ihrem Unternehmen dabei helfen, Anforderungen von Zertifizierungen wie beispielsweise ISO 27001 und TISAX zu erfüllen.

6.2 DSGVO-konforme Datenverarbeitung

Die Europäische Datenschutz-Grundverordnung (DSGVO) ist eine der wichtigsten Errungenschaften für eine selbstbestimmte digitale Identität. Der Schutz der persönlichen Daten ist uns schon immer ein wichtiges Anliegen gewesen. Bei der Nutzung unserer Software und den damit verbundenen Informationen achten wir stets darauf, keine Daten zu erheben und alle notwendigen Daten im Sinne der DSGVO zu verarbeiten.

DSGVO		heylogin	
Art. 5	Grundsätze für die Verarbeitung personenbezogener Daten	Wir achten bei der Verwendung externer Software darauf, dass Datenschutz an oberster Stelle steht. Wir nutzen nur Anbieter mit erweiterten Datenschutzeinstellung, um die maximale Datensicherheit des Nutzers zu garantieren.	✓

Art. 17	Recht auf Löschung	Wir setzen das Recht auf Löschung organisatorisch um. Melden Sie sich bei unserem Support und wir löschen Ihre Daten zum schnellstmöglichen Zeitpunkt.	✓
Art. 20	Recht auf Datenübertragbarkeit	Wir ermöglichen den Export von Daten durch den Nutzer.	✓
Art. 32	Sicherheit der Verarbeitung	Wir erheben personenbezogene Daten nur in besonderen Fällen und verschlüsseln alles, was Rückschlüsse auf die Person zulässt.	✓

6.3 ISO 27001

Die Internationale Organisation für Normung (ISO) entwickelt und veröffentlicht weltweit technische, industrielle und kommerzielle Normen. Die Norm ISO 27001 für Information Security Management Systems (ISMS) bietet einen Rahmen für die Informationssicherheit, der aus 114 Maßnahmen besteht. Um die ISO-27001-Zertifizierung zu erhalten, müssen Unternehmen die Mehrzahl aller Maßnahmen nachweisen.

Während jede Maßnahme wichtige Ziele in Bezug auf die organisatorische Sicherheit und sichere Prozesse enthält, sollten Unternehmen dem Anhang A.9 besondere Aufmerksamkeit widmen. heylogin kann als Technische Maßnahme für die Abschnitte A.9.4.2 und A.9.4.3 eingesetzt werden.

ISO 27001 Maßnahmen		heylogin	
A.9.4.2	**Secure log-on procedures – Sichere Anmeldeverfahren**	In dieser Maßnahme geht es um die Verwendung der Multi-Faktor-Authentifizierung für die sichere Anmeldung an Systemen.	
		Unsere Sicherheitsarchitektur ist immer 2-Faktor-sicher ohne die Nachteile klassischer Verfahren,	✓

		da alle Zugänge mit dem Sicherheitschip des Smartphones Ende-zu-Ende-verschlüsselt sind. Dieser Sicherheitschip bildet damit den 1. Faktor (Besitz) und muss immer auf dem Smartphone selber durch einen 2. Faktor (Biometrie oder PIN) entsperrt werden. Damit wird jeder Zugang zu jeder Webseite 2-Faktor-sicher gespeichert und geschützt.	
		Dadurch dass kein Master-Passwort verwendet wird, entfallen Mitarbeiterschulungen zum Umgang mit dem Passwort-Manager.	✓
A.9.4.3	**Password management system – System zur Verwaltung von Kennwörtern**	In dieser Maßnahme geht es um die Verwaltung von Passwörtern, einschließlich der Fähigkeit, sichere Passwörter zu erstellen. Von der Weitergabe von Passwörtern wird in der ISO-Norm abgeraten.	
		heylogin speichert Passwörter Ende-zu-Ende-verschlüsselt automatisiert und generiert sichere Passwörter für die Account-Registrierung. Passwörter können Mitarbeitern zugewiesen oder in Teams organisiert werden. Des Weiteren kann durch heylogin das Teilen von Zugängen durch Admins kontrolliert und damit unachtsame Herausgeben von Passwörtern unterbunden werden. Durch eine Richtlinie ist es möglich Zugänge zu Teilen ohne die dazugehörigen Passwörter herauszugeben.	✓

6.4 ISO 27002

ISO/IEC 27002 ist ein Standard der ISO-27000-Familie, der *Best Practices* enthält und somit individuell von Organisationen entsprechend den jeweiligen Informationssicherheitsrisiken interpretiert und angewendet werden kann. Diese Flexibilität gibt den Anwendern auf der einen Seite viel Spielraum die passenden Maßnahmen auszuwählen und umzusetzen, auf der anderen Seite ist die ISO 27002 damit für Konformitätsprüfungen ungeeignet. Die Maßnahmen in Anhang A der ISO 27001 sind von der ISO 27002 abgeleitet und mit ihr abgestimmt.

Der Einsatz von heylogin unterstützt Unternehmen bei der Umsetzung der ISO 27002 bei den organisatorischen Maßnahmen (ISO 27002:2022, „organizational controls“, Clause 5) sowie den technischen Maßnahmen (ISO 27002:2022, „technological controls“, Clause 8).

ISO 27002 Maßnahmen 2013	**2022 (Jahr der Veröff.)**		heylogin	
09.2.1	**5.16**	**Identity management**	In dieser Maßnahme geht es um das Identitätsmanagement in Unternehmen.	
		Guidance b)	Mit heylogin haben Entscheider immer die volle Kontrolle welche Logins als „shared identities“ von mehreren Mitarbeiter genutzt werden. Dies erfüllt die Genehmigung und Dokumentationspflichten.	✓
		d)	Logins können jederzeit gelöscht oder einzelnen Mitarbeitern entzogen werden. Dies erfüllt die prozeduralen Anforderungen.	✓
		f)	Eine Nachverfolgbarkeit wird in einer zukünftigen Version von heylogin durch eine Zugriffshistorie abgebildet.	✓

09.2.4, 09.3.1, 09.4.3	**5.17**	**Authentication information**	In dieser Maßnahme geht es um die Speicherung und das Management von Authentisierungsdaten.	
		Guidance „Allocation of authentication information“ a)	heylogin generiert Passwörter für jeden Login während der Registrierung automatisch. Sie sind somit einzigartig für jede Webseite und können nicht erraten werden.	✓
		c)	Wie gefordert, werden Passwörter nie im Klartext übertragen, sondern über heylogin Ende-zu-Ende-verschlüssel zugewiesen oder im Team genutzt.	✓
		d)	Eine Nutzerbestätigung ist in heylogin technisch umgesetzt. Mitarbeiter können den Beitritt zu einem heylogin Team per Klick bestätigen.	✓
		f)	In einer zukünftigen Version von heylogin wird eine bessere Nachverfolgbarkeit durch eine Zugriffshistorie abgebildet.	✓
		User responsibilities a)	Mit heylogin bleiben Passwörter immer verschlüsselt und werden nur mit berechtigten Mitarbeitern geteilt.	✓
		c)	heylogin generiert Passwörter automatisch und erfüllt damit alle Anforderungen in diesem Punkt.	✓
		d)	Durch die Passwortgenerierung sind Passwörter einzigartig.	✓
		Password management system b)	Wie auch in „User responsibilities“ (c) gefordert, werden starke Passwörter nach dem Stand der Technik generiert.	✓
		g)	Passwörter werden beim Einloggen nicht angezeigt. heylogin ersetzt den Loginvorgang auf Webseiten im Browser.	✓

		h)	Passwörter werden nur Ende-zu-Ende-verschlüsselt in heylogin ausgetauscht.	✓
		Other information	heylogin ist als „password vault“ einzustufen. Es schützt und vereinfacht den Umgang mit Passwörtern. Wie im Standard beschrieben werden so Maßnahmen effektiv umgesetzt.	✓
07.2.2	**6.3**	**Information security awareness, education and training**	In dieser Maßnahme geht es um den Einsatz von Weiterbildungsmaßnahmen und Trainings für Mitarbeiter im Kontext der Informationssicherheit.	
			Durch den Einsatz von heylogin entfallen Security Awareness Trainings zu Passwortsicherheit, da diese technisch umgesetzt wird.	✓
09.4.2	**8.5**	**Secure authentication**	In dieser Maßnahme geht es um die Technik und Prozesse der Authentisierung um Zugriffskontrollen umzusetzen.	
		Guidance	Durch heylogin sind Zugänge automatisch hardwaregeschützt und „by default“ 2-Faktor-sicher. Damit ist die geforderte „multi-factor authentication“ für alle Webseiten umgesetzt.	✓
		e)	Zusätzlicher Brute-Force-Schutz auf Seiten des Login-Mechanismus ist nicht notwenig, da heylogin sichere und einzigartige Passwörter generiert und nutzt.	✓
		i)	heylogin ersetzt den Loginvorgang auf Webseiten im Browser. Somit sind Passwörter nicht für den Mitarbeiter sichtbar.	✓
		k)	In heylogin können Geräte jederzeit gesperrt oder entsperrt werden. Eine automatische Sperrung erfolgt am Ende eines Arbeitstages.	✓

6.5 TISAX

Trusted Information Security Assessment Exchange (TISAX) ist ein Prüf- und Austauschverfahren der Automobilbranche und ermöglicht es, den Reifegrad der Informationssicherheit bei potenziellen Partnern zu prüfen. Der Verband der Automobilindustrie (VDA) veröffentlicht das Information Security Assessment (ISA) als Kriterienkatalog für eine TISAX-Prüfung.

heylogin ist eine mögliche Maßnahme um den gewünschten Schutzbedarf im Kriterienkatalog *Informationssicherheit* zu erreichen. Dies gilt besonders für den Bereich des *Identity and Access Management* (VDA ISA Katalog v5.0 Abschnitt 4).

VDA ISA v5.0 Katalog		heylogin	
3.1.4	Inwieweit ist der Umgang mit mobilen IT-Geräten und mobilen Datenträgern gemanagt?	heylogin setzt den Nutzung von Android- oder iOS-Smartphones im Unternehmen voraus. Um die 2-Faktor-Sicherheit zu gewährleisten wird vorausgesetzt, dass eine Displaysperre mit Biometrie oder PIN aktiviert ist.	✓
4.1.2	Inwieweit wird der Zugang von Benutzern zu Netzwerkdiensten, IT-Systemen und IT-Anwendungen gesichert?	Wir haben eine 2-Faktor-Authentifizierung über persönliche Smartphones in unserer Software integriert, um die Sicherheit beim Austausch von vertraulichen und streng vertraulichen Daten zu gewährleisten.	✓
4.1.3	Inwieweit werden Benutzerkonten und Anmeldeinformationen sicher verwaltet und angewandt?	Wir haben eindeutig personalisierte Nutzerkonten, auf die wir durch unser Verschlüsselungsprotokoll keinerlei Zugriff haben.	✓
4.2.1	Inwieweit werden Zugriffsberechtigungen vergeben und gemanagt?	Passwörter sind durch die Verschlüsselung nur dem Nutzer bekannt.	✓

5.1.1	Inwieweit wird die Nutzung kryptografischer Verfahren gemanagt?	Wir verschlüsseln und hashen die zu übertragenden Daten mit mehreren kryptographischen Verfahren und nutzen als Algorithmen XSalsa20+Poly1305 und Curve 25519.	✓
5.1.2	Inwieweit werden Informationen während der Übertragung geschützt?	Durch Ende-zu-Ende Verschlüsselung können nur Sender und Empfänger auf die Daten zugreifen.	✓

Bitte beachten:

Um die TISAX-Anforderungen zu erfüllen, darf die heylogin Team-Funktion nicht verwendet werden. Als Nachweis ist eine organisatorische Lösung möglich, z. B. in Form eines schriftlichen Nachweises.