Inhaltsverzeichnis

1. Setup:Installationsanleitung/Optimierungen/Cronjobs 2
2. Benutzer:Richard.heigl 4
3. Info:Trust and Safety/Cloud - Sicherheit und Zuverlässigkeit 4
4. Info:Trust and Safety/Software - Sicherheit und Zuverlässigkeit 5
5. Info:Trust and Safety/Zertifizierung und Compliance 6

Cronjobs

Versionsgeschichte interaktiv durchsuchen
VisuellWikitext

Version vom 7. August 2023, 19:49 Uhr (Quelltext anzeigen)	**Version vom 10. August 2023, 12:56 Uhr (Quelltext anzeigen)**
Richard Heigl (Diskussion | Beiträge)	Richard Heigl (Diskussion | Beiträge)
K (→Kontinuierliche Verbesserung der bereitgestellten Software)	KKeine Bearbeitungszusammenfassung
Markierung: Visuelle Bearbeitung	Markierung: Visuelle Bearbeitung
← Zum vorherigen Versionsunterschied	Zum nächsten Versionsunterschied →
Zeile 15:	**Zeile 15:**
*'''Hotfix-Fähigkeit''': Durch automatisierte Tests und Auslieferung können wir einen Hotfix innerhalb von 4 Stunden in die Produktionsumgebung übernehmen.	*'''Hotfix-Fähigkeit''': Durch automatisierte Tests und Auslieferung können wir einen Hotfix innerhalb von 4 Stunden in die Produktionsumgebung übernehmen.
==Business Continuity Konzept==	==Business Continuity Konzept==
Folgende Maßnahmen schützen unsere Kunden vor Schäden und Unterbrechungen der Cloud Services :	Folgende Maßnahmen schützen unsere Kunden vor Schäden und Unterbrechungen der Cloud Services:
*Hallo Welt! '''überwacht die Verfügbarkeit und Performance''' der Cloud-Infrastruktur und '''informiert auf einer [https://status.bluespice.com/w/index.php/Main_Page Status-Seite] über den aktuellen Status''' der Services, über Ausfallzeiten und Wartungsfenster.	*Hallo Welt! '''überwacht die Verfügbarkeit und Performance''' der Cloud-Infrastruktur und '''informiert auf einer [https://status.bluespice.com/w/index.php/Main_Page Status-Seite] über den aktuellen Status''' der Services, über Ausfallzeiten und Wartungsfenster.
*Die Dienste werden im Fehlerfall '''automatisch neu gestartet'''.	*Die Dienste werden im Fehlerfall '''automatisch neu gestartet'''.
*Alle '''Daten werden stündlich gesichert'''. Wir sichern 4 Stunden und 7 Tage. Die täglichen Backups werden in einem separaten Rechenzentrum gespiegelt. Die Backups sind verschlüsselt.	*Alle '''Daten werden stündlich gesichert'''. Wir sichern 4 Stunden und 7 Tage. Die täglichen Backups werden in einem separaten Rechenzentrum gespiegelt. Die Backups sind verschlüsselt.
*Hallo Welt! führt '''Desaster- und Recovery-Tests''' für ihre Cloud-Infrastruktur durch; die RTO (Recovery Time Objective) beträgt 4 Stunden.	*Hallo Welt! führt '''Desaster- und Recovery-Tests''' für ihre Cloud-Infrastruktur durch; die RTO (Recovery Time Objective) beträgt 4 Stunden.
*Die '''**Hallo Welt!** überprüft und verbessert''' regelmäßig ihre Sicherheitsmaßnahmen.	*Die **Hallo Welt!** '''überprüft und verbessert''' regelmäßig ihre '''Sicherheitsmaßnahmen'''.
*Hallo Welt! führt ein '''Notfallhandbuch''', das alle existenziellen Bedrohungen für die Infrastruktur und den Umgang damit abdeckt.	*Hallo Welt! führt ein '''Notfallhandbuch''', das alle existenziellen Bedrohungen für die Infrastruktur und den Umgang damit abdeckt.
*Hallo Welt! führt ein '''Risikoregister'''.	*Hallo Welt! führt ein '''Risikoregister'''.

Version vom 10. August 2023, 12:56 Uhr

Hier erklären wir Ihnen die Konzepte unserer Cloud Services.

Inhaltsverzeichnis

1 Sicherheitsprinzipien unserer Cloud Services 3
2 Kontinuierliche Verbesserung der bereitgestellten Software 3
3 Business Continuity Konzept 3
4 Externe Links 4

Sicherheitsprinzipien unserer Cloud Services

- **100 Prozent EU-DSGVO-konform**: Die vollständige Umsetzung des EU-Rechts (v.a. Datensparsamkeit, keine Speicherung außerhalb der EU und nur bei Unternehmen in der EU) ist für uns selbstverständlich. Mehr dazu finden Sie unter Zertifizierung und Compliance.
- **Sichere "Public Cloud"**: Jeder unserer Kunden hat seine eigene Datenhaltung, insbesondere im Dateisystem und in der Datenbank. Die Instanzen teilen sich jedoch die Services, z.B. den Datenbankservice, den Suchservice oder die PDF-Erstellung. Alle genutzten Dienste sind mandantenfähig, so dass sichergestellt ist, dass keine Daten von einer Instanz in die andere gelangen können. Die Cloud wird zentral von Hallo Welt! administriert. Updates werden zentral eingespielt. Die Instanzen teilen sich die Server-Ressourcen.
- **Authentifizierung und Autorisierung**: Die Abfrage von Berechtigungen und die Vergabe von Benutzergruppenrechten wird von BlueSpice durch eine Reihe von Maßnahmen unterstützt. Eine genauere Beschreibung finden Sie hier: Software - Sicherheit und Zuverlässigkeit.
- **Zugriffsbeschränkung für Hallo Welt! bzw. deren Dienstleister**: Als Betreiber der Cloud muss Hallo Welt! in der Lage sein, den unterbrechungsfreien Betrieb der Cloud-Infrastruktur sowie der Kundeninstanzen dauerhaft zu gewährleisten. Dazu kann es notwendig sein, sich auf die Server aufzuschalten. Wenn wir aber Zugriff auf die Server haben, haben wir theoretisch auch Zugriff auf die Kundendaten. Daher ist dieser Zugriff streng reglementiert und auf sehr wenige Mitarbeiter mit hoher Vertrauenswürdigkeit und Verschwiegenheitspflicht beschränkt. Externe Dienstleister von Hallo Welt! haben zu keinem Zeitpunkt Zugriff auf die Daten in der Cloud.
- **Verschlüsselung**: Wir unterstützen software- und serverseitige Verschlüsselungsverfahren. Lesen Sie hierzu mehr unter: Software - Sicherheit und Zuverlässigkeit.

Kontinuierliche Verbesserung der bereitgestellten Software

Unsere Software BlueSpice wird ständig weiterentwickelt und verbessert. Um diese Änderungen zeitnah in die Cloud ausliefern zu können, setzen wir folgende Mechanismen ein:

- **Continuous Delivery**: Änderungen in der Cloud werden regelmäßig wöchentlich durchgeführt. Bei Bedarf erfolgen Updates auch häufiger.
- **Automatisierte Tests von Software und Infrastruktur**: Jede Änderung am System wird durch automatisierte Tests abgesichert.
- **Betrieb einer Qualitätssicherungsumgebung**: Jede Änderung am System wird in einer baugleichen Qualitätssicherungsumgebung vorgetestet und erst nach erfolgreichem Test in die Produktionsumgebung eingespielt.
- **Automatisierte Auslieferung**: Änderungen werden automatisiert über unsere Deployment-Queue ausgeliefert. Im Fehlerfall kann so schnell auf eine Vorgängerversion zurückgegriffen werden.
- **Hotfix-Fähigkeit**: Durch automatisierte Tests und Auslieferung können wir einen Hotfix innerhalb von 4 Stunden in die Produktionsumgebung übernehmen.

Business Continuity Konzept

Folgende Maßnahmen schützen unsere Kunden vor Schäden und Unterbrechungen der Cloud Services:

- Hallo Welt! **überwacht die Verfügbarkeit und Performance** der Cloud-Infrastruktur und **informiert auf einer Status-Seite über den aktuellen Status** der Services, über Ausfallzeiten und Wartungsfenster.
- Die Dienste werden im Fehlerfall **automatisch neu gestartet**.

- Alle **Daten werden stündlich gesichert**. Wir sichern 4 Stunden und 7 Tage. Die täglichen Backups werden in einem separaten Rechenzentrum gespiegelt. Die Backups sind verschlüsselt.
- Hallo Welt! führt **Desaster- und Recovery-Tests** für ihre Cloud-Infrastruktur durch; die RTO (Recovery Time Objective) beträgt 4 Stunden.
- Die Hallo Welt! **überprüft und verbessert** regelmäßig ihre **Sicherheitsmaßnahmen**.
- Hallo Welt! führt ein **Notfallhandbuch**, das alle existenziellen Bedrohungen für die Infrastruktur und den Umgang damit abdeckt.
- Hallo Welt! führt ein **Risikoregister**.

Externe Links

Beachten Sie ergänzend unsere Information auf der Produkt-Website:

- BlueSpice: Cloud Hosting
- Häufig gestellte Fragen: Cloud

Benutzer:Richard.heigl: Unterschied zwischen den Versionen

Aktuelle Version vom 6. Dezember 2021, 14:43 Uhr (Quelltext anzeigen)
Richard Heigl (Diskussion | Beiträge)
(create user page)

(kein Unterschied)

Aktuelle Version vom 6. Dezember 2021, 14:43 Uhr

Info:Trust and Safety/Cloud - Sicherheit und Zuverlässigkeit: Unterschied zwischen den Versionen

Freigegeben:11:47, 19. Okt. 2022 / Revision vom: 11:47, 19. Okt. 2022
Versionsgeschichte interaktiv durchsuchen
VisuellWikitext

Version vom 19. Oktober 2022, 11:26 Uhr (Quelltext anzeigen)	**Version vom 19. Oktober 2022, 11:47 Uhr (Quelltext anzeigen)**
Margit Link-Rodrigue (Diskussion | Beiträge)	Margit Link-Rodrigue (Diskussion | Beiträge)
(Leere Seite erstellt)	Keine Bearbeitungszusammenfassung
Markierung: Visuelle Bearbeitung	Markierung: Visuelle Bearbeitung
	Zum nächsten Versionsunterschied →
Zeile 1:	**Zeile 1:**
	Diese Seite befindet sich im Aufbau.

Version vom 19. Oktober 2022, 11:47 Uhr

Diese Seite befindet sich im Aufbau.

Info:Trust and Safety/Software - Sicherheit und Zuverlässigkeit: Unterschied zwischen den Versionen

Freigegeben:17:35, 3. Feb. 2023 / Revision vom: 17:34, 3. Feb. 2023
Versionsgeschichte interaktiv durchsuchen
VisuellWikitext

Version vom 3. Februar 2023, 17:21 Uhr (Quelltext anzeigen)	**Version vom 3. Februar 2023, 17:34 Uhr (Quelltext anzeigen)**
Richard Heigl (Diskussion | Beiträge)	Richard Heigl (Diskussion | Beiträge)
KKeine Bearbeitungszusammenfassung	Keine Bearbeitungszusammenfassung
Markierung: Visuelle Bearbeitung	Markierung: Visuelle Bearbeitung
← Zum vorherigen Versionsunterschied	Zum nächsten Versionsunterschied →
Zeile 10:	**Zeile 10:**
* '''Sichere Verschlüsselungsverfahren auf der Grundlage von Industriestandards:''' Hier wird z.B. die Kommunikation zwischen Anwendung und Benutzer durch TLS abgesichert und Passwörter durch Hashing sicher in der Datenbank gespeichert. Für die Benutzerauthentifizierung kann auf bewährte Standards wie SAML oder OpenID Connect gesetzt werden.	* '''Sichere Verschlüsselungsverfahren auf der Grundlage von Industriestandards:''' Hier wird z.B. die Kommunikation zwischen Anwendung und Benutzer durch TLS abgesichert und Passwörter durch Hashing sicher in der Datenbank gespeichert. Für die Benutzerauthentifizierung kann auf bewährte Standards wie SAML oder OpenID Connect gesetzt werden.
* '''Modularität''': Die Software ist modular und objektorientiert aufgebaut. Einzelne Funktionen können bei Bedarf deaktiviert und individuelle Anforderungen einfach umgesetzt werden. Auch kompatible Erweiterungen aus dem MediaWiki-Ökosystem, die nicht direkt Bestandteil von BlueSpice sind, können bei Bedarf nachinstalliert werden (On Premises).	* '''Modularität''': Die Software ist modular und objektorientiert aufgebaut. Einzelne Funktionen können bei Bedarf deaktiviert und individuelle Anforderungen einfach umgesetzt werden. Auch kompatible Erweiterungen aus dem MediaWiki-Ökosystem, die nicht direkt Bestandteil von BlueSpice sind, können bei Bedarf nachinstalliert werden (On Premises).
* '''Interoperabilität''': BlueSpice stellt verschiedene Schnittstellen sowie Import- und Exportfunktionen zur Verfügung, um die Wiki-Software mit anderen Systemen zu verbinden. Über eine gut dokumentierte Web API (u.a. REST) können Aufgaben automatisiert und der Datenaustausch zwischen verschiedenen internen IT-Systemen realisiert werden. Ein einfaches XML-basiertes Datenformat ermöglicht den Im- und Export von Wiki-Seiteninhalten und eignet sich z.B. für die Migration bestehender Dokumentenbestände. Darüber hinaus stehen verschiedene **Authentifizierungsanbieter** (Active Directory/LDAP, SAML, Open ID Connect) zur Auswahl, die eine nahtlose Integration von BlueSpice in die eigene IT-Infrastruktur ermöglichen.	* '''Interoperabilität''': BlueSpice stellt verschiedene Schnittstellen sowie Import- und Exportfunktionen zur Verfügung, um die Wiki-Software mit anderen Systemen zu verbinden. Über eine gut dokumentierte Web API (u.a. REST) können Aufgaben automatisiert und der Datenaustausch zwischen verschiedenen internen IT-Systemen realisiert werden. Ein einfaches XML-basiertes Datenformat ermöglicht den Im- und Export von Wiki-Seiteninhalten und eignet sich z.B. für die Migration bestehender Dokumentenbestände. Darüber hinaus stehen verschiedene **Authentifizierungssysteme** (Active Directory/LDAP, SAML, Open ID Connect) zur Auswahl, die eine nahtlose Integration von BlueSpice in die eigene IT-Infrastruktur ermöglichen.
Siehe auch:	Siehe auch:

Version vom 3. Februar 2023, 17:34 Uhr

Hinweis: Die Seite wird aktuell erweitert

Prinzipien der Softwareentwicklung

Die Softwareentwicklung von BlueSpice basiert auf einer Reihe wichtiger Prinzipien:

- **Cloud-First-Ansatz**: Die Software wird für den Einsatz in unserem Cloud-Angebot entwickelt und regelmäßig auch für On-Premises-Installationen veröffentlicht.
- **Security-by-Default**: Alle relevanten Sicherheitseinstellungen sind bereits in der Grundkonfiguration der Software und unserer Services aktiviert.
- **Herstellerunabhängigkeit** durch Open-Source-Entwicklung: Hallo Welt! ist zwar alleiniger Hersteller der Softwaredistribution BlueSpice, der von Hallo Welt! produzierte Code wird jedoch unter aktiver Beteiligung der der MediaWiki-Community in den öffentlichen Repositories der Wikimedia Foundation entwickelt und ist somit frei zugänglich. Damit ist sichergestellt, dass der Support für die Nutzer der Software nicht nur durch Hallo Welt!, sondern auch durch andere Dienstleister geleistet werden kann (Vermeidung eines Lock-in-Effekts).
- **Einsatz quelloffener Standards, Technologien und Formate**: Hallo Welt! setzt auf offene Standards , die besonders leicht zugänglich, erweiterbar und einsetzbar sind. Die nötige Server-Infrastruktur kann vollständig mit Open-Source-Software bereitgestellt werden (z. B. Linux-Betriebssysteme oder MariaDB als Datenbanksystem). Die Software BlueSpice basiert auf und nutzt verschiedene offene Standards (z. B. TLS, TCP/IP, IPv6 als Netzwerkprotokoll für die Kommunikation, sowie HTML, JavaScript, CSS und XML für die Darstellung und Funktion). Es verwendet standardisierte Zeichensätze und Kodierungen und unterstützt die Verwendung offener Formate wie PNG, Ogg, SVG, CSV oder MathML. Und natürlich unterstützt BlueSpice einheitliche Standards zur Beschreibung von Metadaten wie RDF.
- **Sichere Verschlüsselungsverfahren auf der Grundlage von Industriestandards:** Hier wird z.B. die Kommunikation zwischen Anwendung und Benutzer durch TLS abgesichert und Passwörter durch Hashing sicher in der Datenbank gespeichert. Für die Benutzerauthentifizierung kann auf bewährte Standards wie SAML oder OpenID Connect gesetzt werden.
- **Modularität**: Die Software ist modular und objektorientiert aufgebaut. Einzelne Funktionen können bei Bedarf deaktiviert und individuelle Anforderungen einfach umgesetzt werden. Auch kompatible Erweiter ungen aus dem MediaWiki-Ökosystem, die nicht direkt Bestandteil von BlueSpice sind, können bei Bedarf nachinstalliert werden (On Premises).
- **Interoperabilität**: BlueSpice stellt verschiedene Schnittstellen sowie Import- und Exportfunktionen zur Verfügung, um die Wiki-Software mit anderen Systemen zu verbinden. Über eine gut dokumentierte Web API (u.a. REST) können Aufgaben automatisiert und der Datenaustausch zwischen verschiedenen internen IT-Systemen realisiert werden. Ein einfaches XML-basiertes Datenformat ermöglicht den Im- und Export von Wiki-Seiteninhalten und eignet sich z.B. für die Migration bestehender Dokumentenbestände. Darüber hinaus stehen verschiedene Authentifizierungssysteme (Active Directory /LDAP, SAML, Open ID Connect) zur Auswahl, die eine nahtlose Integration von BlueSpice in die eigene IT-Infrastruktur ermöglichen.

Siehe auch:

- Verena Hösl: BlueSpice Produktentwicklung –von der Planung bis zur Dokumentation, BlueSpice Summit 2022.
- Open Source Business Alliance: Sicherheit: Open Source Software und proprietäre Software im Vergleich, 21. Juni 2022.

Info:Trust and Safety/Zertifizierung und Compliance: Unterschied zwischen den Versionen

Freigegeben:22:19, 9. Nov. 2022 / Revision vom: 22:18, 9. Nov. 2022
Versionsgeschichte interaktiv durchsuchen
VisuellWikitext

Version vom 9. November 2022, 22:08 Uhr (Quelltext anzeigen)	**Version vom 9. November 2022, 22:18 Uhr (Quelltext anzeigen)**
Richard Heigl (Diskussion | Beiträge)	Richard Heigl (Diskussion | Beiträge)
Keine Bearbeitungszusammenfassung	Keine Bearbeitungszusammenfassung
Markierung: 2017-Quelltext-Bearbeitung	Markierung: Visuelle Bearbeitung
← Zum vorherigen Versionsunterschied	Zum nächsten Versionsunterschied →

Zeile 29:	**Zeile 29:**
Hallo Welt! hat einer Anti-Bestechungs- und Korruptionsrichtlinie eingeführt. Diese Richtlinie dient der Einhaltung und Aufrechterhaltung unserer Null-Toleranz-Position gegenüber Bestechung und Korruption.	Hallo Welt! hat einer Anti-Bestechungs- und Korruptionsrichtlinie eingeführt. Diese Richtlinie dient der Einhaltung und Aufrechterhaltung unserer Null-Toleranz-Position gegenüber Bestechung und Korruption.
Sie dient auch als Informationsquelle und Orientierungshilfe für diejenigen, die für Hallo Welt! arbeiten, um Bestechungs- und Korruptionsfragen zu erkennen und damit umzugehen, sowie ihre Verantwortung zu verstehen. Die Richtlinie ist auf der BlueSpice-Seite veröffentlicht: [https://bluespice.com/de/vertraege-und-richtlinien/ **BlueSpice-Produktseite**]	Sie dient auch als Informationsquelle und Orientierungshilfe für diejenigen, die für Hallo Welt! arbeiten, um Bestechungs- und Korruptionsfragen zu erkennen und damit umzugehen, sowie ihre Verantwortung zu verstehen. Die Richtlinie ist auf der BlueSpice-Seite veröffentlicht: [https://bluespice.com/de/vertraege-und-richtlinien/ **Rechtliches**]
[[en:Info:Trust_and_Safety/Certification_and_compliance]]	[[en:Info:Trust_and_Safety/Certification_and_compliance]]

Version vom 9. November 2022, 22:18 Uhr

Zertifizierungen und Standards

Hallo Welt! orientiert sich an Normen und unterstützt standardisierte Verfahren und führt diese auch selbst ein:

- Unsere **Cloud-Rechenzentren** sind ISO/IEC 27001:2005 zertifiziert. Siehe hierzu Hetzner Online Zertifizierung.
- Hallo Welt! arbeitet prozessorientiert. Wir ein internes **Organisationshandbuch** und ein intern **dokumentiertes Prozessmanagement**, das sich an der Norm ISO 9001 orientiert.
- Weiter orientiert sich Hallo Welt! als Softwarehersteller am **BSI-Standard für IT-Grundschutz**:
  - **Notfallmanagement**: Wir führen ein Notfallhandbuch, in dem alle existenziellen Bedrohungen der Infrastruktur und der Umgang damit festgehalten sind
  - **Risikomanagement**: Wir führen ein Risikoregister.
  - **Business Continuity:** Unsere Maßnahmen für das Disaster Recovery siehe unter Cloud - Sicherheit und Zuverlässigkeit.
  - **Protokollierung, Monitoring und Detektion** von sicherheitsrelevanten Ereignissen: Wir haben ein Verzeichnis aller Incidents.
  - **Audits**: Alles das wird regelmäßig überprüft.
- Hallo Welt! hat ein **Cyber Essentials Zertifikat.**
- Hallo Welt! **plant für 2023 eine Zertifizierung nach ISO/IEC 27001:2005** und hat alle notwendigen Prozesse gemäß den BSI Standards für Cloud Computing implementiert.

Benutzerfreundlichkeit und Barrierefreiheit

Wir entwickeln BlueSpice so, dass die Bedienbarkeit der Software möglichst einfach, einheitlich und intuitiv ist.

Unsere Software-Entwicklung bemüht sich sehr, den internationalen Standard WCAG 2.1 und den Europäischen Standard EN 301 549 Accessibility requirements suitable for public procurement of ICT products and services in Europe, - V3.1.1 (2019-11) zu beachten und umzusetzen.

Die Ergebnisse der internen Tests zur Barrierefreiheit können jederzeit hier eingesehen werden (auf Englisch):

- Freiwilliger Konformtätsbericht (Vorlage: ITI VPAT)
- Teststatus der einzelnen BlueSpice / MediaWiki-Erweiterungen

Wir sind dankbar für jeden Hinweis unserer Kunden und Anwender, der die kontinuierliche Verbesserung der Barrierefreiheit ermöglicht.

Anti-Bestechungs- und Korruptionsrichtlinien

Hallo Welt! hat einer Anti-Bestechungs- und Korruptionsrichtlinie eingeführt. Diese Richtlinie dient der Einhaltung und Aufrechterhaltung unserer Null-Toleranz-Position gegenüber Bestechung und Korruption.

Sie dient auch als Informationsquelle und Orientierungshilfe für diejenigen, die für Hallo Welt! arbeiten, um Bestechungs- und Korruptionsfragen zu erkennen und damit umzugehen, sowie ihre Verantwortung zu verstehen. Die Richtlinie ist auf der BlueSpice-Seite veröffentlicht: Rechtliches