Kanton St.Gallen
Bildungsdepartement

Amt für Mittelschulen

Informationssicherheits-Konzept

Lernnavi

Inhaltsverzeichnis

1 Generelle Anmerkungen

1.1 Beschreibung

Lernnavi ist ein Online-Lernfördersystem für die Fachbereiche Deutsch und Mathematik auf der Sekundarstufe II. Es wird als Hilfsmittel zur Erreichung eines Teils der basalen fachlichen Kompetenzen für die allgemeine Studierfähigkeit eingesetzt. Lernnavi ist ein intelligentes, adaptives Fördersystem, welches den Schülerinnen und Schülern ihr individuelles Leistungsniveau aufzeigt und ihnen passend zu ihren Fähigkeiten Aufgaben zuweist.

Lernnavi basiert auf den Methoden und Technologien des maschinellen Lernens. Dazu erfasst das System verschiedene Daten, welche Rückschlüsse auf das Kompetenzniveau der einzelnen Schülerin und des einzelnen Schülers zulassen. Die Daten sind personenbezogen und fallen damit unter das Datenschutzgesetz.

1.2 Zweck des Dokuments

Das IS-Konzept legt die nötigen Angaben zur Erhaltung und Verbesserung der Informationssicherheit und des Datenschutzes fest. Es fasst die Aspekte der Informationssicherheit im Projekt zusammen.

Die Aspekte des Datenschutzes werden separat im Dokument Datenschutzkonzept Lernnavi (vgl. 4, Dokument 13) behandelt.

1.3 Gültigkeit des Dokuments

Die Gültigkeit dieses IS-Konzepts beträgt ein Jahr. Zum Zeitpunkt der Erstellung dieses Konzepts waren verschiedene betriebliche und organisatorische Aspekte noch nicht abschliessend definiert. Der Grund dafür liegt in der Neuartigkeit dieses Lernfördersystems, sowie darin, dass es von einem Startup-Unternehmen entwickelt wird, welches in Bezug auf betriebliche Prozesse ebenfalls in der Entwicklung steht. Das vorliegende IS-Konzept trägt diesem Umstand Rechnung. Mit zunehmender Erfahrung während der Pilotphase und der Einführung und Etablierung einer Betriebsorganisation, muss auch das IS-Konzept weiterentwickelt werden.

2 Management Summary

2.1 Allgemeines

Basierend auf den bestehenden Vorgaben des Kantons St. Gallen wurden die minimalen Anforderungen zum Schutzbedarf entsprechend umgesetzt. (Merkblatt «Klassifizierung Informatiksicherheit» - Schutzbedarfsanalyse)

Im Rahmen von Informationssicherheit und Datenschutz sind die rechtlichen Grundlagen, Verordnungen und Dienstanweisungen geprüft und die wichtigsten Punkte definiert. Durch technische und organisatorische Massnahmen sind diese Vorgaben adressiert, um den Anforderungen an die Bearbeitung von Personendaten und von besonders schützenswerten Daten gerecht zu werden. Eine Vorabkontrolle und eine damit verbundene weiterführende Risikoanalyse bzw. Schutzbedarfsanalyse wurden nicht durchgeführt. Im Projekt wurde dies nachträglich vollzogen. In rechtlicher Hinsicht sind die Aspekte einer datenschutzrechtlichen Vorabkontrolle somit sinngemäss berücksichtigt.

2.2 Restrisiken

Die Restrisiken sind insbesondere auf den noch niedrigen Reifegrad des Gesamtsystems (neue Applikation, neue Methoden, neuer Hersteller - Startup) zurückzuführen. Die Restrisiken können jedoch in Kauf genommen werden. Mit dem Ausbau und der Weiterentwicklung des Systems einhergehen muss aber eine kontinuierliche Entwicklung in den folgenden Bereichen:

- Systemdokumentation

- Qualitätssicherung
- Monitoring von Administratorenzugriffen
- Vergabe und Verwaltung von Systemzugriffsrechten im Entwicklungsteam
- Notfallkonzeption

3 Rechtsgrundlagen, Informationssicherheit und Datenschutz

3.1 Rechtliche Grundlagen

Folgende rechtliche Grundlagen gelten im Kontext von Lernnavi:

- Datenschutzgesetz des Kantons St.Gallen (DSG; sGS 142.1)
- Verordnung über die Informatiksicherheit des Kantons St.Gallen vom 24. Februar 2004 (sGS 142.21)
- Dienstanweisung über Einsatz und Verwendung von Informatikmitteln vom 25. August 2009 der Regierung des Kantons St.Gallen

3.2 Übersicht der wichtigsten Punkte für Informationssicherheit und Datenschutz

Thema	Beschreibung
Geltungsbereich Datenschutzgesetz	Bearbeitung von Personendaten (Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen) durch öffentliche Organe (Kanton, Gemeinden usw.).
Bearbeitung von Personendaten und besonders schützenswerten Daten	Gesetzliche Grundlage: Art. 3 ff DSG, Bearbeitung setzt Rechtsgrundlage voraus oder ist zur Erfüllung einer gesetzlichen Aufgabe erforderlich. Qualifizierte gesetzliche Voraussetzungen für Bearbeitung besonders schützenswerter Personendaten, Öffentliches Organ ist verantwortlich für organisatorische und technische Massnahmen zur Sicherung der Daten vor Verlust und missbräuchlicher Verwendung.
Anonymisierung von Daten	Ein Rückschluss auf die einzelne Person ist im konkreten Fall nicht mehr möglich. Anonymisierung ist eine verhältnismässige Massnahme im Datenschutzrecht und ist nach Möglichkeit (Bsp. Reporting) anzuwenden.
Zugriffskontrolle / Zugriffs-konzept	Ein Zugriffskonzept und technische Massnahmen sind entsprechend auszuarbeiten und einzuführen, um den Zugriff auf die Daten zu regeln und zu schützen. Die Berechtigungs- und Rollenkonzepte müssen verwaltungsintern gewährleisten, dass die Datenbearbeitung durch die hierfür zuständigen Personen erfolgt und dass diese Berechtigungen restriktiv erteilt und periodisch überprüft werden.
Datenbearbeitung von Dritten	Gesetzliche Grundlage: Art. 9 DSG Die Verantwortung im Falle einer Bearbeitung durch Dritte für die Einhaltung der datenschutz- und sicherheitsrelevanten Vorschriften verbleibt in jedem Fall beim Outsourcinggeber. Dieser muss die Einhaltung der Vereinbarung kontrollieren und allenfalls geeignete Massnahmen ergreifen, um die Vorschriften durchzusetzen.

Tabelle 1: Wichtige Punkte für Informationssicherheit

4 Verzeichnis der sicherheitsrelevanten Dokumente

Ref.	Titel
01	Kanton St.Gallen: Datenschutzgesetz
02	Schweizerische Eidgenossenschaft: Bundesgesetz über den Datenschutz
03	Europäische Union: Datenschutz-Grundverordnung
04	Kt. SG, Bildungsdepartement (2019): Datenschutz und Informationssicherheit in der Schule, Handreichung https://www.sg.ch/bildung-sport/volksschule/rahmenbedingungen/rechtliche-grundlagen/Datenschutz.htm
05	Kt. SG, Regierung (2009): Dienstanweisung über Einsatz und Verwendung von Informatikmitteln
06	Kt. SG, Dienst für Informatikplanung (2016): Merkblatt der Klassifizierung
07	Kt. SG, Dienst für Informatikplanung (2019): Klassifizierung Informatiksicherheit, Checkliste
08	Kt. SG, Dienst für Informatikplanung (2019): Massnahmenkatalog Informatiksicherheit
09	Kt. SG (2004): Verordnung über die Informationssicherheit
10	Kt. SG (2007): Konzept Informatiksicherheit
11	KOM SG (2016): Sicherheitsvorschriften KOM SG
12	Kt. SG, Dienst für Informatikplanung (2019): KTSG Anwendungsintegration – Merkblatt für Anwendungslieferanten – neue AD-Strategie
13	Kt. SG, Amt für Mittelschulen (2020): Datenschutzkonzept Lernnavi
14	Kt. SG, Amt für Mittelschulen (2020): Betriebskonzept Lernnavi

Tabelle 2: Verzeichnis der sicherheitsrelevanten Dokumente

5 Einstufung

Gemäss dem Merkblatt für die Klassifizierung der Informatiksysteme und -anwendungen vom Dienst für Informatikplanung des Kantons St. Gallen (vgl. 4, Dokument 06) wird Lernnavi wie folgt klassifiziert:

- Vertraulichkeit Stufe V: Vertrauliche Daten und Personendaten
- Verfügbarkeit: Stufe 1: Daten mit mittlerer Verfügbarkeit (Tolerierte Ausfallzeit 1-3 Tag, Wiederbeschaffung der Daten im Normalfall möglich, bei Datenverlust)

6 Sicherheitsrelevante Systembeschreibung

6.1 Ansprechpartner / Verantwortlichkeiten

Wer	Name
Anwendungsverantwortliche	Tina Cassidy, Amt für Mittelschulen
Inhaber der Daten	Schülerinnen und Schüler
Systembeschreiber	Taskbase AG
Projektleiterin	Barbara Bitzi, Amt für Mittelschulen
Betriebsleiterin	Nicole Menzel, Amt für Mittelschulen/Pädagogische Hochschule St.Gallen
ISBD	Marc Hänggi
DSBO	Heidi Roth
Benutzerkreis	Schülerinnen, Schüler, Lehrpersonen, Autorinnen, Autoren

Tabelle 3: Ansprechpartner

6.2 Beschreibung des Gesamtsystems

Lernnavi besteht aus zwei voneinander getrennten Applikationen. Die Benutzerplattform stellt den Schülerinnen und Schülern das Login und die Funktionalitäten zum Durchführen von Übungen und Tests, Übersichten zur Auswertung sowie ein Forum zur Verfügung. Die Analyse der Eingaben der Schülerinnen und Schüler wird auf einer zweiten Applikation, der Autorenplattform, durchgeführt. Diese Unterteilung hat folgenden Grund:

Die Auswertung der Eingaben der Schülerinnen und Schüler geschieht mittels rechenleistungsintensiver Methoden des maschinellen Lernens. Um auch bei einer Vielzahl von Schülerinnen und Schülern eine gute Reaktionszeit des Systems sicherzustellen, muss die Rechenleistung skalierbar sein. Gleichzeitig darf das System nicht zu hohe Kosten generieren, damit möglichst alle Schulen davon profitieren können. Diese beiden Kriterien werden von grossen, meist über die ganze Welt verteilten Rechenzentren (Public Cloud) am besten erfüllt. In den meisten Fällen befinden sich diese Infrastrukturen nicht in der Schweiz und unterliegen auch nicht der Schweizerischen Gesetzgebung.

Die Funktionalitäten des Lernfördersystems Lernnavi sind deshalb auf zwei Applikationen mit je einer eigenen Datenbank aufgeteilt. Die Benutzerplattform mit den personenbezogenen Daten ist auf einem Server in der Schweiz konfiguriert, welcher die geforderten Datenschutzrichtlinien sicherstellen kann. Taskbase benutzt die Dienstleistungen des Schweizer Cloud-Anbieters Exoscale um die Lernnavi Serverinfrastruktur zu betreiben. Die Autorenplattform für die rechenleistungsintensiven Berechnungen arbeitet ausschliesslich mit anonymisierten Daten und kann somit in einer Public Cloud betrieben werden. Damit wird eine hohe Wirtschaftlichkeit bei gleichzeitiger Gewährleistung des Datenschutzes erzielt.

6.2.1 Authentifizierungsmethode

Für den Zugriff auf die Benutzerplattform und die Autorenplattform (Kommunikation Client-Server) wird das HTTPS Protokoll verwendet. Die Benutzeraccounts sind passwortgeschützt. Für die Rollen *Student*, *Teacher* und *Editor* (vgl. Kap. 6.2.6) gelten folgende Regeln für das Passwort: Mindestens 8 Zeichen, davon mindestens eine Zahl und ein Sonderzeichen.

Die Komplexität dieser Regeln entsprechen nicht den Vorgaben gemäss Massnahmenkatalog Informatiksicherheit (vgl. 4, Dokument 08), weil sich ein komplexes Passwort insbesondere bei Schülerinnen und Schülern kontraproduktiv auswirken kann. Passwörter werden in diesem Fall oft auf Zettel geschrieben.

Für die Rolle *Administrator* gelten die Regeln gemäss Massnahmenkatalog Informatiksicherheit (vgl. 4, Dokument 08): Mindestens 12 Zeichen lang, komplex und jährlich sowie unmittelbar nach

einem Weggang eines Wissensträgers zu ändern. Für unterschiedliche Funktionen werden unterschiedliche Passwörter verwendet. Eine 2FA ist bei Serverzugriffen von Administratoren auf allen Instanzen vollständig konfiguriert.

6.2.2 Datenbank

Die Datenbanken der Benutzer- sowie der Autorenplattform sind redundant ausgelegt und durch eine Firewall geschützt, so dass nur die jeweilige Applikation (Middleware Server) darauf zugreifen kann. Die Datenbanken befinden sich auf verschlüsselten Harddisks (Data at rest). Für die Verschlüsselung wird der Standard AES-256 verwendet.

6.2.3 Anonymisierung

Die Benutzerprofile der Schülerinnen und Schüler sind nur in den Datenbanken der Benutzerplattform gespeichert. Die Interaktionsdaten der Schülerinnen und Schüler sind nur in den Datenbanken der Autorenplattform abgelegt. Für die Kommunikation zwischen der Benutzerplattform und der Autorenplattform wird eine zufällig generierte Benutzer-ID verwendet. Die Informationen auf der Autorenplattform sind damit nur der Benutzer-ID, aber keinem Benutzerkonto zuweisbar. Dadurch sind sie auf der Autorenplattform anonymisiert.

6.2.4 Monitoring und Logging

Ein Monitoring der Systemzugriffe wird in einer ersten Phase nicht realisiert. Die Detaillierung der Systemzugriffe wird zu einem späteren Zeitpunkt definiert.

6.2.5 Gewaltentrennung

Das Betriebskonzept (vgl. 4, Dokument 14) regelt die Verantwortlichkeiten und Zuständigkeiten.

6.2.6 Rollenkonzept

Für die Zuordnung von Rollen und Zugriffsrechten wird ein Role Based Access Control System verwendet. Darin sind folgende Rollen definiert:

Rolle	**Beschreibung**	**Zugewiesene Rolle im «Role Based Access Control System» des Lernnavi** (siehe dazu auch Informationssicherheitskonzept, vgl. Kap. 4, Dokument 13)
Schülerin und Schüler	Die eigentlichen Nutzerinnen und Nutzer des Systems. Sie können auf der Benutzerplattform ein persönliches Konto einrichten. Sie können Aufgaben lösen und am Forum teilnehmen.	STUDENT
Lehrperson	Die jeweiligen Lehrpersonen der Schülerinnen und Schüler. Sie können für die Schülerinnen und Schüler Lektionen zusammenstellen und am Forum teilnehmen.	TEACHER
Autorin und Autor	Fachpersonen, welche die Aufgaben erstellen und die anonymisierten Feedbacks der Schülerinnen und Schüler analysieren. Sie haben Zugriff auf alle Funktionen der Autorenplattform.	EDITOR
Super User	Auf Lernnavi gut ausgebildete Personen, welche als erste Anlaufstelle für Fragen von Schülerinnen, Schüler und Lehrpersonen agieren. Sie haben einen Lehreraccount für Lernnavi.	TEACHER
Administratorin und Administrator	Personen der Betreiberin (Betriebsteam) des Lernnavi, welche das System betreiben. Sie können EDITOR und TEACHER Rollen vergeben. Sie können sogenannte «Tenants» für neue Schulen registrieren	ADMINISTRATOR ROOT (Oberstes Administratoren Account, mit welchen Administratoren Rollen vergeben werden können)

Tabelle 4: Rollen in Lernnavi

Weitere Angaben zu Rollen siehe Dokument Betriebskonzept Lernnavi (vgl. 4, Dokument 14).

6.2.7 Sicherheitslücken

Das System wird täglich auf Sicherheitslücken überprüft. Dies geschieht automatisiert durch einen externen Provider. Während des Scans sucht die Crashtest Security Suite nach den folgenden Arten von Schwachstellen und Sicherheitsproblemen:

✓Server Version Fingerprinting ✓ Web Application Version Fingerprinting ✓ CVE-Vergleich ✓ Heartbleed ✓ ROBOT ✓ BREACH ✓ BEAST ✓ Alte SSL/TLS Version ✓ SSL/TLS Cipher Order ✓ SSL/TLS Perfect Forward Secrecy ✓ SSL/TLS Session Resumption ✓ SSL/TLS secure algorithm ✓ SSL/TLS key size ✓ SSL/TLS trust chain ✓ SSL/TLS expiration date ✓ SSL/TLS revocation (CRL, OCSP) ✓ SSL/TLS OCSP Stapling ✓ Security Headers ✓ Content-Security-Policy Headers ✓ Portscan ✓ Boolean-basierte blinde SQL Injection ✓ Zeitbasierte blinde SQL Injection ✓ Fehlerbasierte SQL Injection ✓ UNION Query-basierte SQL Injection ✓ Stacked Queries SQL Injection ✓ Out- of-band SQL Injection ✓ Reflected Cross-Site Scripting (XSS) ✓ Stored Cross-Site Scripting (XSS) ✓ Cross-Site Request Forgery (CSRF) ✓ File Inclusion ✓ Directory Fuzzer ✓ File Fuzzer ✓ Command Injection ✓ XML External Entity Processing (XXE)

6.2.8 Backup

Jede Nacht wird ein Backup sämtlicher Informationen erstellt. Die Backups werden nach 30 Tagen gelöscht. Für die Benutzerplattform und die Autorenplattform werden separate Backups erstellt. Taskbase arbeitet nach dem Continuous Integration Prinzip und benutzt dazu ein auf Gitlab basierendes Framework, das Taskbase erlaubt, Rollbacks zu alten Versionen der Applikation per Knopfdruck auszuführen. Allerdings ist dies nur ohne Datenverlust möglich, falls das Datenbankschema in der Zwischenzeit nicht verändert wurde. Restore Tests führt Taskbase nicht systematisch aus, allerdings wird das Prozedere in unregelmässigen Abständen auf der Development Umgebung getestet. Alle Daten sind in zwei verschiedenen MySQL Datenbanken abgespeichert, von denen Taskbase jeweils jede Nacht einen verschlüsselten Dump abspeichert.

6.2.9 Support und Wartungsprozesse

Siehe Dokument Betriebskonzept Lernnavi (vgl. 4, Dokument 14)

6.3 Beschreibung der zu bearbeitenden Daten

Siehe Dokument Datenschutzkonzept Lernnavi (vgl. 4, Dokument 03)

6.4 Architekturskizze

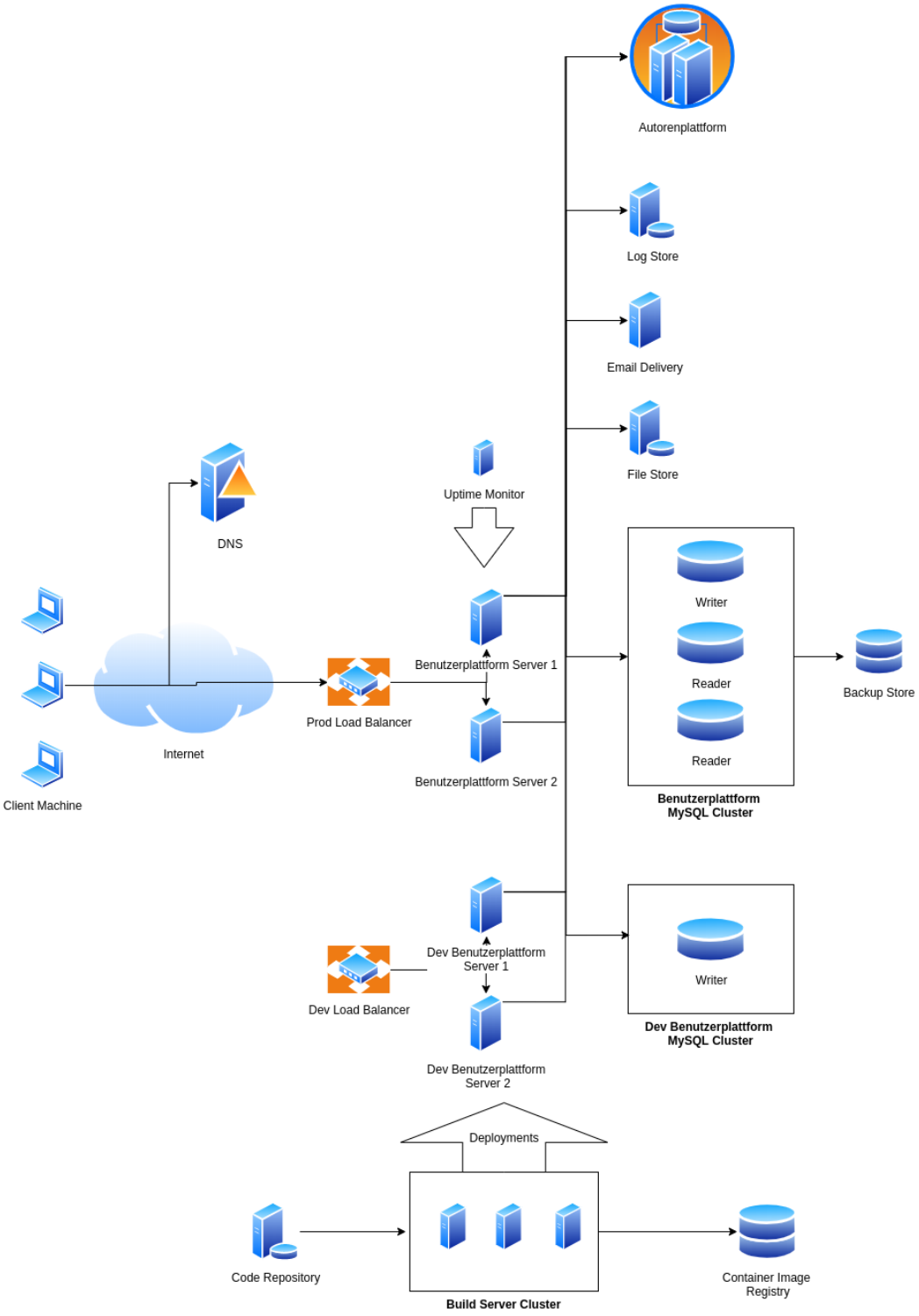

Abbildung 1: Architekturskizze

E-Mail Delivery: E-Mails werden versendet für Passwort-Zurücksetzungen und um Anmeldungen zu verifizieren.

Die Kommunikation erfolgt verschlüsselt mit StartTLS/TLS (keine E2E Verschlüsselung)

File Store: Wird verwendet, um Bilder für die Aufgaben abzuspeichern. Die Autoren benutzen einen HTML Editor, der es ihnen erlaubt Bilder einzufügen. Diese Bilder landen auf diesem File Store. Als File Store dient AWS S3.

6.5 Beschreibung der zugrundeliegenden Technik

Die Applikation für die Benutzerplattform läuft auf mehreren Middleware Servern. Wie viele Server eingesetzt werden hängt von der Nachfrage ab. Ein Load Balancer verteilt die Anfragen automatisch auf die vorhandenen Server. Die Datenbank der Benutzerplattform wird auf einem separaten Server betrieben.

Die Benutzerplattform benötigt diverse zusätzliche Systeme. Diese kommunizieren miteinander über eine REST-Schnittstellen. Die Kommunikation zwischen Benutzerplattform und Autorenplattform wird ebenfalls über diese Schnittstelle sichergestellt.

Parallel zum produktiven System wird für Testzwecke ein zweites System inklusive Load Balancer betrieben (Dev Load Balancer). Das Testsystem hat eine eigene Datenbank (verwendet keine Daten aus der Produktion) und greift nie auf das produktive System und dessen Datenbank zu. Es dient beispielsweise dazu, neue Versionen und Updates zu testen.

6.5.1 Load Balancer

Der Load Balancer verteilt die Last der Benutzer auf die verschiedenen Middleware Server und funktioniert als Firewall um einfache DNS-Angriffe, die das System mit Überlastung zum Absturz bringen würden, abzuwehren. Zudem hostet der Load Balancer das SSL Zertifikat und ist dafür verantwortlich, dass die Verbindung mit dem Client verschlüsselt wird.

6.5.2 Middleware Server

Der Middleware-Server wird als Docker Image ausgerollt und benötigt ein Linux Betriebssystem mit einem Docker Daemon.

6.5.3 Datenbank

Die Datenbank ist MySQL Version 5.7 und besteht aus einem Hauptserver und einem Replikat.

6.5.4 Build Server

Die Build Server kompilieren und testen den Programmcode und erstellen daraus die Docker Images, die im Docker Image Store abgelegt werden. Zudem ist der Build Server dafür verantwortlich, den Middleware Server auszurollen.

6.5.5 Netzwerk

Da Lernnavi auch in anderen Kantonen genutzt wird, ist es nicht ins kantonale Netzwerk des Kanton St.Gallen integriert.

7 Risikoanalyse und Schutzmassnahmen

Lernnavi erfasst und verarbeitet personenbezogene Daten der Schülerinnen und Schüler. Damit fällt es unter das Datenschutzgesetz. Mit den erfassten Interaktionsdaten wird mit Methoden des maschinellen Lernens ein Score der Schülerin oder des Schülers erstellt. Dieser Score gibt Auskunft über den persönlichen Lernfortschritt und den Lernstand. Es ist zu erwarten, dass mit der weiteren technologischen Entwicklung die Qualität der Analyse der Interaktionsdaten stetig verbessert wird. Damit wächst auch deren Aussagekraft zum persönlichen Lernverhalten der Schülerinnen und Schüler. Deshalb muss sichergestellt sein, dass die Schülerinnen und Schüler die Kontrolle über diese sensitiven Daten haben. Lehrpersonen sehen die Resultate der Lern- und Testsession der Schülerinnen und Schüler nur, wenn diese sie freischalten. Interaktionsdaten werden ausschliesslich in anonymisierter Form erfasst. Möchten die Schülerinnen und Schüler Zugriff auf ihre gesamten Daten oder sollen die Daten gelöscht werden, können sie eine Supportanfrage senden.

Die erfassten Interaktionsdaten können zu Forschungszwecken weiterverwendet werden. Dazu müssen die Daten gemäss Datenschutzgesetz zwingend anonymisiert sein.

7.1 Restrisiken

Nach der Realisierung sämtlicher vorsorglichen Massnahmen bleiben Restrisiken bestehen. Es sind dies:

Nr.	Risikobeschreibung	Wert	Einschätzung/Massnahmen
1	Unbeabsichtigte oder beabsichtigte Deanonymisierung der Daten, weil Personen (beispielsweise Softwareentwickler) auf beide Plattformen (Benutzerplattform und Autorenplattform) zugreifen können.	Mittel	Mittelfristig: keine Personen, welche gleichzeitig auf die Benutzerplattform sowie die Autorenplattform zugreifen können. Regelung über Betriebs-/Outsourcing Vereinbarung;
2	Fehlerhafte Resultate durch Systemfehler, weil System neu, Methoden neu und kein ausgeprägter, organisatorischer Reifegrad des Herstellers (Taskbase), da Startup.	Mittel	Mittelfristige Nachführung der Systemdokumentation; Mittelfristige Einführung von Qualitätsstandards und -prozessen;
3	Verlust von Daten	Tief	Risiko wird getragen, Verlust von Daten von einem Tag werden in Kauf genommen;
4	Absichtliche oder unabsichtliche Manipulation / Löschen von Daten durch Administratoren.	Tief	Ein Monitoring der Administratorenzugriffe wird spätestens nach erfolgter Pilottests realisiert. Regelung über Betriebs-/Outsourcing Vereinbarung.
5	Das Fehlen einer Webapplication-Firewall (WAF) und der Konfiguration. Diese würde den HTTP-Verkehr von und zu Lernnavi monitoren, filtern oder blockieren.	Mittel	Der Fokus sollte in erster Instanz auf der Entwicklung der sicheren Applikation liegen, im Weiteren ist jedoch die Installation einer WAF unabdingbar und sollte den Schutz der Webapplikation zusätzlich vor Angriffen (Denial-of-Service oder SQL-Injection) absichern.

Tabelle 5: Restrisiken

8 Wiederherstellung des Geschäftsbetriebs

Ein Notfallkonzept existiert noch nicht und muss zu einem späteren Zeitpunkt erstellt werden.

9 Einhaltung / Überprüfung / Abnahme der Schutzmassnahmen

Das Betriebskonzept (vgl. 4, Dokument 14) definiert den Prozess zur Prüfung (Test) und Einführung von Updates und neuen Releases.

Das System wird mittels automatisierten Tests durch eine Drittfirma täglich auf Sicherheitslücken geprüft.

10 Ausserbetriebnahme

Die Ausserbetriebnahme von Lernnavi ist im Rahmenvertrag zwischen dem AMS und Taskbase geregelt und folgt den ordentlichen Vorgaben bezüglich Aufbewahrung und Entsorgung von Daten und Hardware. Die Verantwortung liegt beim Betriebsausschuss Lernnavi.