eXaminer

P042 - Informationssicherheits- und Datenschutzkonzept eXaminer

Klassifizierung	EXTERN
Status	Finale Version
Datum	16.02.2021
Autor/Autoren	Melanie Widmer, Florian Bentele

Inhalt

1 Projekt eXaminer

Der eXaminer ist eine Prüfungsplattform, in der Prüfende online Fragen erstellen, diese sortieren und in Prüfungen zusammenstellen können. Die Prüfungen können mit dem eXaminer durchgeführt und ausgewertet werden. Der eXaminer wird als Software as a Service (SaaS) betrieben.

Lehrpersonen erarbeiten über Jahre hinweg Prüfungen, zusammengestellt aus einzelnen Prüfungsfragen und -aufgaben. Dieser Fundus blieb bisher in den Computern der Lehrpersonen verschollen.
Der eXaminer hat das Ziel Prüfungsfragen strukturiert zu erfassen und somit eine durchsuchbare Sammlung von Fragen und Musterlösungen zu ermöglichen. Mehrere Lehrpersonen können sich zusammen als Gruppe verbinden und ihre eigenen Fragen mit anderen Lehrpersonen teilen sowie deren Fragen in den eigenen Fragenkatalog importieren. So entsteht eine grössere Vielfalt an Prüfungsfragen und die Qualität der Prüfungen wird gesteigert. Die Zusammenarbeit bietet einen zweiten grossen Vorteil: die Zeitersparnis beim Erstellen und Korrigieren einer Prüfung.
Die Prüfungen aus dem eXaminer können als PDF heruntergeladen und ausgedruckt oder gleich online in einem Webbrowser durchgeführt werden.
Dieses Informations- und Datenschutzkonzept (ISDS-Konzept) bezieht sich einerseits auf die Daten von Lehrpersonen im Zusammenhang mit der Erfassung der Prüfungsfragen und andererseits mit den Daten von Lernenden, wenn diese die Prüfung online durchführen.

2 Management Summary

2.1 Zweck des Dokuments

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

2.2 Gültigkeit des Dokuments

Die Gültigkeit dieses ISDS-Konzepts beträgt 2 Jahre. Danach ist eine Aktualisierung nötig.

2.3 Allgemeines

Der Umgang mit Daten aus dem Bildungssektor ist besonders sensibel. Die Daten geben Auskunft über Personen die möglicherweise minderjährig sind und die sich nicht gegen deren Erfassung aussprechen können. Nicht zuletzt aus diesen Gründen ist der Schutz dieser Daten oberste Priorität bei der Entwicklung und im Betrieb des eXaminers.
Wir verfolgen eine strikte und transparente Informationspolitik und arbeiten ausschliesslich mit Schweizer Unternehmen und Dienstleistern zusammen. Die gesamte Entwicklung, Betrieb, Support, Hosting und Backups des eXaminers befinden sich in der Schweiz und werden ausschliesslich aus der Schweiz betreut.

Pro Kunde (Schule oder Institution) wird eine eigene Datenbankinstanz verwendet. Die Daten sind daher pro Kunde isoliert. Innerhalb der Applikation können die Daten nur durch die explizite Freigabe eingesehen werden. Daten von Lernenden sind nur durch die Lehrperson einsehbar, die die Prüfung erstellt und durchgeführt hat.

2.4 Zusammenfassung Restrisiken

Weitergabe von Zugangsdaten an Dritte

Wenn eine Lehrperson das eigene Kennwort an Dritte weitergibt, können diese Zugriff auf die Daten dieser Lehrperson ausüben und sämtliche, für diese Lehrperson freigegeben Daten einsehen und kopieren.

Hacken von unsicheren Kennwörtern
Wenn eine Lehrperson ein schwaches Kennwort verwendet, kann dieses von einem Angreifer eruiert werden. Der Zugriff auf alle Daten, die für diese Lehrperson freigegeben sind ist dadurch gewährt.

Datenverlust durch Systemausfall
Trotz regelmässigen Backups bleibt ein kleines Restrisiko durch einen Datenverlust, z.B. aufgrund von defekter Hardware oder durch einen Fehler in der Software. Dieses Risiko wird reduziert durch die das standortunabhängige Backup der Daten.

2.5 Abschliessende Bemerkungen

Alle schützenswerten Daten innerhalb des eXaminers werden aus technischer Sicht vor unberechtigtem Zugriff geschützt. Die grösste Gefahr eines Verlustes liegt bei den Anwendenden und der Kennwortsicherheit.

3 Verzeichnis der sicherheitsrelevanten Dokumente

Dokumententyp	Titel
Gesetz	SR 152.1 Bundesgesetz über die Archivierung (Archivierungsgesetz, BGA) SR 235.1 Bundesgesetz über den Datenschutz (DSG)
Übergeordnete Sicherheitskonzepte	Sicherheitskonzept oder Datenschutzbedingungen der Institution oder der Schule
AGBs der Hostingpartnerin	https://www.hostpoint.ch/hostpoint/kontakt-agb.html
AGB eXaminer	https://www.examiner.cloud/wp-content/uploads/2020/04/AGBs.pdf

4 Einstufung des Schutzobjekts

Gemäss der Schutzbedarfsanalyse P041 verwendet oder verarbeitet der eXaminer Persönlichkeitsprofile.

4.1 Gespeicherte Daten

Personendaten
Von Lehrpersonen sowie Schuladmins werden Vorname, Name und E-Mailadresse zu Korrespondenz- und Zugriffszwecken gespeichert. Von den Lernenden wird ebenfalls der eingegebene Name sowie die E-Mailadresse gespeichert.

Inhaltliche Daten
Das System speichert Ihre Fragen, deren Lösungen, Ihre Übungen und Prüfungen sowie die gewählten Bewertungsmethoden.

Prüfungen und Noten
Bei Prüfungen werden alle von den Lernenden gegebenen Antworten, ihre Bewertung und die Schlussnote gespeichert.

Statistische Daten
Wir erheben Daten zu analytischen Zwecken (z.B. Nutzungsdauer, Nutzungshäufigkeit). Diese Daten werden anonym erhoben.

4.1.1 Datenaufbewahrung
Im Prinzip bewahren wir Daten so lange auf, wie die Geschäftsbeziehung dauert. Bei Beendigung der Geschäftsbeziehung werden alle Daten einer Institution oder einer mit Einzellizenz arbeitenden Person gelöscht oder auf Wunsch ausgehändigt.

5 Sicherheitsrelevante Systembeschreibung
Im Folgenden sind die System-Elemente beschrieben, welche als Sicherheitsrelevant eingestuft werden.

5.1 Gesamtsystem
Der eXaminer ist cloudbasiert. Alle Daten, die im System gespeichert werden, sind auf dem Server des Hosters abgelegt. Die Hostingpartnerin, die Hostpoint AG, hat ihren Firmenstandort in der Schweiz. Die Hostpoint AG hat ausserdem alle ihre Server in der Schweiz und diese werden nach aktuellen Sicherheitsstandards betrieben.
Die Daten verlassen währen der Nutzung die Server nicht, sämtliche Daten werden nicht im Browser zwischengespeichert.

5.1.1 Rollenkonzept
Folgende Rollen werden für das System des eXaminers vergeben:

Anonym: Schüler*innen loggen sich anonym in das System ein. Sie haben keinen Zugriff auf Daten. Einzige Ausnahme bildet die freigegebene Prüfung sowie das eigene Prüfungsresultat. Anonyme Benutzer haben keinen Zugriff und können Daten weder sehen noch bearbeiten. Einzige Ausnahme sind die freigegebenen Prüfungen, welche durch eine eindeutige und kryptische URL aufgerufen werden können. Diese URL ist nicht bekannt und wird dritten niemals bekannt gegeben. Die URL ist zu jedem Zeitpunkt nur der Lehrperson und dem Lernenden bekannt.

Lehrperson: Hat Zugriff auf Prüfungsfragen, Schüler*innendaten (Name, Vorname, Mailadresse) sowie die Prüfungsresultate der eigenen Schüler*innen. Um Zugriff auf Prüfungsfragen anderer Lehrpersonen zu haben müssen diese vom / von der Urheber*in explizit freigegeben werden.

Schuladmin (bei Einzellizenz nicht vorhanden): Kann Benutzer und Gruppen verwalten und Fragen freigeben/löschen. Hat Zugriff auf alle Prüfungsfragen, sowie alle Prüfungsresultate.

Admin: Kann jede andere Rolle annehmen. Hat somit Zugriff auf Schüler*innendaten, Prüfungsfragen und Prüfungsresultate. Diese Rolle ist nur für den technischen Support und wird im Regelfall keinem Benutzer zugewiesen.

Rolle	Zugriff auf	Kein Zugriff auf
Anonym	Eigene Prüfung mit expliziter URL, eigenes Prüfungsresultat	Jegliche Daten
Lehrperson	Eigene Prüfungsfragen, Prüfungsresultate der eigenen	Nicht freigegebene Prüfungsfragen anderer Lehrpersonen,

	Prüfung. Schüler*innedaten der eigenen Schüler*innen	Prüfungsresultate anderer Lehrpersonen, Daten von Schüler*innen anderer Lehrpersonen
Schuladmin	Prüfungsfragen aller Lehrpersonen,	Prüfungsresultate anderer Lehrpersonen oder deren Lernenden
Admin	Sämtliche Daten	

Zugriff auf Daten der Lernenden
Abgeschlossene Prüfungen mit Daten von Lernenden können nicht von Dritten eingesehen werden. Die Lehrperson kann die korrigierte Prüfung mit Rückmeldungen an den Lernenden senden (E-Mail). Der Lernende kann mittels einer kryptischen URL die eigene Prüfung, resp. die Prüfungsergebnisse einsehen.

Login / Authentisierung
Das Login für den Schuladmin wird vom Admin erstellt. Der Schuladmin vergibt persönliche Logins für Lehrpersonen.
Sämtliche Zugriffe auf das System sind nur mit Authentifizierung möglich.

Lehrpersonen, Schuladmin und Admins loggen sich über einen persönlichen Login ein. Das Passwort dafür setzen sie selber.

Schüler*innen die sich anonym einloggen bekommen einen persönlichen Link der Ihnen den Zugriff auf die Prüfung ermöglicht. Sie geben eine Korrespondenzadresse ein, über welche zu einem späteren Zeitpunkt das Prüfungsresultat vermittelt wird.

5.1.2 Backup
Es werden automatisch Backups der Daten durchgeführt. Das Backupkonzept kopiert sämtliche Daten einmal täglich vom Rechenzentrum an einen zweiten, unabhängigen Standort in der Schweiz. Die Backups werden für 30 Tage aufbewahrt und danach endgültig gelöscht. Ein Abweichendes Backupkonzept kann mit der alea iacta digital vereinbart werden. Die Daten aus dem Backup werden nur nach Rücksprache mit dem Kunden verwendet und sind nur für den Notfall zur Wiederherstellung des Systems.

5.1.2.1 Support- und Wartungsprozesse
Der eXaminer wird laufend weiterentwickelt. Updates und neue Funktionen werden regelmässig auf dem System installiert. Über die geplanten Wartungsarbeiten und Änderung werden die Kunden direkt informiert.

Supportanfragen werden über die E-Mail Adresse support@examiner.cloud innerhalb eines Arbeitstages beantwortet. Weiter gibt es eine Benutzerdokumentation, resp. Anleitung in PDF-Form und online auf http://www.examiner.cloud/dokumentation/

6 Risikoanalyse und Schutzmassnahmen
Die Risikoanalyse wird aufgrund der geringen Komplexität des Projektes in diesem Dokument abgehandelt.

6.1 Mögliche Risikofaktoren
Ausfall oder Störung der Stromversorgung oder von Kommunikationsnetzen

Die Gefahr eines Ausfalls ist immer vorhanden. Die Serverlandschaft auf dem das System betrieben wird, ist redundant aufgebaut. Den Auswirkungen eines Ausfalles wird mit regelmässigen Backups des Systems (vgl. 5.1.2) entgegengewirkt. Das Kommunikationsnetz (Internet Zugriff) liegt in der Verantwortung des Kunden.

Ausfall oder Störung von Dienstleistern

Als externer Dienstleisterin ist nur unsere Hosting-Partnerin integriert. Bei Störung in deren Systeme ist die Software nicht benutzbar. Durch die regelmässigen Backups sowie der Serversicherheit der Hosptiont AG ist hier die Gefahr des Datenverlusts minimal.

Softwareschwachstelle oder -Fehler

Der eXaminer ist eine Eigenproduktion der alea iacta digital GmbH, deren Qualität den höchsten Standards entspricht. Bei der Konzeption und Umsetzung wird mit grösster Sorgfalt vorgegangen. Trotz dem strengen Test-Prozess kann es zu Fehlern kommen. Derzeit sind keine groben Mängel oder Fehler bekannt, gerne nehmen wir Rückmeldungen diesbezüglich entgegen unter support@examiner.cloud.

Unberechtigte oder fehlerhafte Nutzung, Missbrauch von Berechtigungen

Berechtigungen können missbraucht werden. In einem Schulhaus / einer Institution erstellt deshalb nur der Schuladmin Profile für Lehrpersonen. Er oder sie weiss, wer auf welche Prüfungen und Daten Zugriff hat. Berechtigungen werden nur personenbezogen ausgestellt.

Datenmissbrauch

Ein Missbrauch personenbezogener Daten kann aufgrund zweier Szenarien entstehen: ein Missbrauch der Berechtigung oder ein unberechtigter verschafft sich Zugang zu den Daten.
Ersteres wird durch die gezielte Vergabe von Profilen eingedämmt. Zugriff eines Unberechtigten kann ausgelöst werden durch mangelnde Passwortsensibilität bei den Nutzern. Das Hacken kurzer oder unsicherer Passwörter ist grundsätzlich sehr einfach. Unsichere Passwörter sollen vermieden werden. Der eXaminer erfordert derzeit eine Kennwortlänge von mindestens 8 Zeichen, Sonderzeichen oder Zahlen sind derzeit nicht erforderlich aber empfohlen.

Fehlende oder mangelnde Abgrenzung/Isolierung der verschiedenen Datenverarbeitungen

Jede Institution hat ein eigens für die Institution aufgesetztes System. Hier ist die fehlende oder mangelnde Abgrenzung eine minimale Gefahr. Der Austausch der Fragen unter den Lehrpersonen ist sogar ein zentrales Element für den eXaminer.
Bei der Einzellizenz wurden sämtliche Massnahmen ergriffen, die Daten zu isolieren und das Restrisiko ist aufgrund der Konstellation des Systems sehr gering