WHITEPAPER ÜBER SICHERHEIT

Warum wir bei Studytube **Informationssicherheit wichtig finden**

Version 2.0

STUDYTUBE

Inhalt

Einleitung

Durch ständige Weiterbildung und Entwicklung bemühen unsere Nutzer und Mitarbeitenden sich darum, ihre Arbeit immer nach bestem Vermögen ausführen zu können. Dieses Prinzip gilt auch für unsere Backend-Prozesse, insbesondere in Bezug auf die Sicherheit und den Schutz Ihrer Daten. Darum sind wir stolz, dass wir nach ISO 27001 zertifiziert sind.

Neben der Mitarbeiterentwicklung bilden das Vertrauen unserer Nutzer und Kunden sowie die Sicherheit von Informationen die Grundlage unseres Leistungsangebots. Studytube arbeitet kontinuierlich an der Verbesserung der Informationssicherheit. Dies war immer schon ein wesentlicher Aspekt aller Prozesse bei Studytube. Mit dem Wachstum unseres Unternehmens und Kundenbestands ist der Bedarf an einem stärker formalisierten Informationssicherheitsmanagementsystem (ISMS) immer dringlicher geworden.

In den letzten Jahren haben wir unsere Verfahren und Richtlinien dokumentiert, wobei auch regelmäßige Kontrollen und Prüfungen festgelegt wurden. Außerdem haben wir unsere Systeme und Ressourcen überprüft und den Verantwortlichen spezifische, dokumentierte Zuständigkeiten zugewiesen. Schließlich haben wir einen Risikomanagementprozess eingeführt, der uns bei der Ausrichtung unserer Bemühungen um die Verbesserung und Implementierung von Informationssicherheitskontrollen hilft. Das alles mit dem Ziel, Ihre Daten bestmöglich zu schützen.

Ein Managementsystem gemäß ISO 27001 hilft uns, Vorschriften wie zum Beispiel denen der DSGVO zu entsprechen, und gewährleistet, dass wir unsere vertraglichen Verpflichtungen gegenüber unseren Kunden und Lieferanten erfüllen.

Auf den folgenden Seiten finden Sie einen Überblick über alle organisatorischen und technischen Maßnahmen, die Studytube in Bezug auf die Informationssicherheit ergriffen hat.

3. **Anwendungssicherheit**

Studytube stellt sicher, dass Nutzende der Plattform auf genau die Daten zugreifen können, für die sie eine Zugriffsberechtigung haben. Das Sicherheitsmodell funktioniert folgendermaßen:

- Die Plattform hat eine komplexe Struktur auf der Grundlage von Berechtigungen, die auf drei Informationssäulen aufbaut: Personen, Lerneinheiten und Budgets. Nur Inhaber bestimmter Rollen haben jeweils Zugang zu ein, zwei oder allen Säulen. Der Zugriff zu Personen ist je nach dem Team, in dem jemand arbeitet, auf die Daten bestimmter Nutzender begrenzt. Der Zugriff auf Lerneinheiten kann nach den Berechtigungen zum Anzeigen, Bearbeiten, Teilen von oder Zugreifen auf die mit der betreffenden Lerneinheit verbundenen Nutzerdaten differenziert werden. Der Zugriff auf Budgets ist von Freigaberegeln abhängig.

4. **Internetsicherheit**

- Alle Verbindungen zu und von unserem Dienst verwenden HTTPS mit dem Protokoll TLS 1.2 (oder falls möglich neuer), 2048-bit-RSA-Schlüssel and AES-Verschlüsselung, sofern vom Client unterstützt (was bei den meisten modernen Clients der Fall ist). Zum Schutz gegen XSS-Angriffe und Man-in-the-middle-Angriffe verwenden wir eine Content-Security-Policy (CSP) und HSTS-Header.

- Die älteren und schwächeren Protokolle TLS 1.1 und SSL wurden deaktiviert.

- Wir nutzen AWS Security Groups, die den Zugang zum Webserver auf bestimmte Protokolle beschränken.

- Alle Nutzereingaben werden vor Verarbeitung bestätigt. Besonderes Augenmerk gilt der Verhinderung von Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) und SQL-Injection.

- Wir sehen uns regelmäßig die OWASP Top 10 an und betrachten die von OWASP bereitgestellten Regeln als wesentliches Element für die Entwicklung sicherer Software.

5. Schutz **vor Malware**

- Von Nutzern hochgeladene Dateien werden beim Hochladen automatisch auf Malware geprüft und, falls Malware gefunden wird, abgelehnt.

- Malware-Definitionen werden regelmäßig automatisch aktualisiert.

6. Authentifizierung **und Passwörter**

- Die API-Authentifizierung von Studytube basiert auf OAuth 2.0. Die Zugriffstokens sind 100 Byte lang, werden mit dem Pseudozufallsgenerator für Byte-Sequenzen von OpenSSL erzeugt und haben eine Lebensdauer von einer Stunde, wonach sie erneuert werden müssen.

- Alle aktiven Zugriffstokens werden widerrufen, wenn ein Nutzer sein Passwort ändert.

- Für Single Sign-Ons kann SAML 2.0 verwendet werden.

- Geräte können fernabgemeldet werden.

- Passwords werden unter Verwendung des BCrypt-Algorithmus als Salted Hashes gespeichert, sodass Studytube die tatsächlichen Passwörter nicht kennt.

- Hat ein Nutzer sein Passwort vergessen, kann er es zurücksetzen lassen. Auf Anfrage wird dann ein geheimer Link zur Zurücksetzung des Passworts an die primäre E-Mail-Adresse des betreffenden Nutzers gesandt.

- E-Mail-Adressen müssen mittels eines geheimen Tokens bestätigt werden, ehe sie als primäre E-Mail-Adressen verwendet werden können.

- Passwörter werden von Studytube nie auf dem Gerät des Nutzers oder im Browser gespeichert. Stattdessen wird ein OAuth-Token sicher gespeichert.

- Auf mobilen Geräten wird das Token gelöscht, sobald der Nutzer sich abmeldet oder die App deinstalliert.

- Authentifizierungstokens laufen automatisch ab, wenn sie längere Zeit nicht verwendet werden.

- Alle internen Administratoren von Studytube verwenden MFA, um auf die Studytube-Plattform zuzugreifen.

- Benutzerschlüssel/Passwörter für die AWS-Infrastruktur werden regelmäßig gewechselt. Das Studytube-Login ist auf Anwendungsebene gegen Brute-Force-Attacken geschützt (durch Whitelisting von bestimmten Logins und IP-Adressen).

7. **Verschlüsselung**

- Daten werden während der Übertragung und im Ruhezustand verschlüsselt.
- Zur Kommunikation über ein öffentliches Netz wird HTTPS mit TLS 1.2 oder neuer (sofern vom Client unterstützt) verwendet. RSA-Schlüssel sind 2048 Bit lang.
- Das ältere, schwächere SSL-Protokollwurde deaktiviert.
- Kundendaten werden im Ruhezustand mit dem AES-256-Algorithmus verschlüsselt.
- Passwörter werden durch den hochsicheren Bcrypt-Algorithmus als Hashes gespeichert.

8. **E-Mail-Schutz**

- Ausgehende Transaktions-E-Mails werden von Mailgun, einem nach ISO 27001:2017 zertifizierten E-Mail-Zustelldienst, verarbeitet.
- Alle ausgehenden E-Mails erhalten eine DKIM-Signatur.
- Absenderfälschung wird mittels SPF verhindert.

9. Schutz der Server und Infrastruktur

- Die Produktionsumgebungen sind in mehrere sichere Zonen unterteilt, wobei der Datenverkehr zwischen den Zonen durch Firewall-Regeln geschützt ist.
- Für den Zugang zu den Produktionsumgebungen ist eine AWS-SSM-Verbindung mit verpflichtender Zwei-Faktor-Authentifizierung erforderlich.
- Auf das Zugangsmanagement wird das Least-Privilege-Prinzip angewendet. Folglich wird nur einer begrenzten Anzahl an Senior-Systemingenieuren Zugang zu den Servern in den Produktionsumgebungen gewährt.
- Alle Dienste sind durch Firewalls geschützt, die nur absolut notwendigen (Web-)Datenverkehr zulassen.
- Die Server von Studytube werden durch ein zentralisiertes Konfigurationsmanagementsystem bereitgestellt, das eine für alle Server einheitliche, sichere Konfiguration garantiert. Auf alle Konfigurationsdaten wird eine Versionskontrolle angewendet.
- Sicherheitskritische Patches werden innerhalb von 24 Stunden nach ihrem Verfügbarwerden installiert.
- Durch die verwendeten Lastverteiler sind die Studytube-Server automatisch gegen L3-, L4- und L7-DdoS-Angriffe geschützt.

10. **Protokollierung und Überwachung**

- Alle Nutzervorgänge in der Anwendung werden in einer zentralisierten Protokolldatei erfasst.
- Sicherheitsrelevante Server-Protokolldateien werden zentralisiert gespeichert und unterliegen automatisierten Analysen und Alarmmeldungen.
- 24/7-Überwachung und -Alarmierung gewährleisten, dass die Systemingenieure von Studytube bei Dienstunterbrechungen schnell reagieren können.

11. **Datenzentren**

- Datenzentren, die Studytube hosten, sind nach ISO 27001:2017 zertifiziert.
- Das primäre Datenzentrum von Studytube in der EU wird von Amazon Web Services betrieben und be indet sich in Frankfurt, in Deutschland.
- Der physische Zugang zu Datenzentren und Servern ist auf autorisierte Mitarbeitende der Datenzentren begrenzt

12. **Notfallwiederherstellung, Sicherung und Redundanz**

- Studytube garantiert eine Verfügbarkeit von 99,8 %, ausgenommen planmäßiger Wartungsfenster.

- Alle kritischen Dienste sind redundant eingerichtet, um eine hohe Verfügbarkeit zu garantieren, in den meisten Fällen mit vollautomatischer Ausfallsicherung.

- Alle Kundendaten werden mehrmals täglich gesichert. Die Sicherungskopien werden einen Monat lang aufbewahrt, sodass die Daten im Notfall wiederhergestellt werden können.

- Der Notfallwiederherstellungsplan von Studytube hilft bei der schnellen Wiederherstellung von Diensten im Notfall.

13. **Sicherheit während der Entwicklung**

- Die Entwicklungsumgebungen von Studytube sind von den Test- und Produktionsumgebungen getrennt.
- Produktionsdaten werden nie zu Testzwecken verwendet.
- Produktionsdaten werden nie aus der Produktionsumgebung in Testumgebungen übertragen.
- Bei jeder Änderung am Studytube-Code werden automatisierte Testsuiten ausgeführt.
- Änderungen werden erst dann umgesetzt, wenn alle Tests erfolgreich durchlaufen wurden. Zusätzlich werden in einer isolierten, für normale Nutzer nicht zugänglichen Umgebung manuelle Tests und eine Qualitätssicherung durchgeführt.
- Alle Entwickler sind gut ausgebildet und verfügen über umfangreiche Kenntnisse im Bereich der Anwendungssicherheit.
- Alle Änderungen am Studytube-Code werden einem Peer-Review durch Senior-Entwickler unterzogen. Die Anwendung wird entsprechend der besten branchenüblichen Praxis entwickelt und es werden Maßnahmen zur Vorbeugung gegen unter anderem die in den OWASP Top 10 aufgeführten Schwachstellen getroffen.

14. **Sicherheitsprüfungen, Penetrationstests und automatisierte Tests**

- Ein unabhängiges Sicherheitsunternehmen führt mindestens einmal jährlich Penetrationstests durch.
- Mit täglichen automatisierten SSL-Servertests wird sichergestellt, dass unsere SSL-Konfiguration immer den Industriestandards entspricht.
- Die Zugangskontrollen der Anwendung werden automatisierten Tests unterzogen, die nach jeder Änderung und jedem Release durchgeführt werden.
- Alle Änderungen an der Anwendung werden einer Reihe von API-Tests und Integrationstests sowie Unit-Tests und einer statischen Analyse unterzogen.

15. **Organisation und Management**

- Periodisch finden Risikobewertungen und Business-Impact-Analysen statt.
- Das ISMS wird wie von der ISO 27001:2017 vorgeschrieben jährlich sowohl intern als extern geprüft.
- Mit einer Schulung zum Informationssicherheitsbewusstsein wird sichergestellt, dass alle Mitarbeitenden sich der Sicherheitsrisiken und -kontrollen bewusst sind.
- Mitarbeitende mit Zugang zu Kundendaten werden vor ihrer Einstellung überprüft.

  Entwickler müssen vor ihrer Einstellung nachweisen können, dass sie über fundiertes Wissen über Sicherheitsthemen verfügen.
- Zum Schutz sensibler Daten müssen Mitarbeitende von Studytube bei ihrer Einstellung eine Verschwiegenheitserklärung unterschreiben.
- Eine Clean-Desk- und Clear-Screen-Policy gewährleisten die Vertraulichkeit in den Büros von Studytube.
- Arbeitsstationen von Mitarbeitenden müssen durch starke Passwörter, Festplattenverschlüsselung und eine automatische Bildschirmsperre gesichert sein.

- Die Passwortrichtlinie von Studytube erfordert von den Mitarbeitenden die Verwendung von starken, einzigartigen Passwörtern für alle genutzten Systeme und wo möglich Zusatzmaßnahmen wie zum Beispiel eine Zwei-Faktor-Authentifizierung.

- Vertraulichkeit, Integrität und Verfügbarkeit sensibler Informationen werden durch Richtlinien zur Einstufung von Informationen in Kombination mit dokumentierten Verfahren zum Umgang mit Informationen und Ressourcen gewährleistet.

- Alle Richtlinien haben jeweils einen definierten Verantwortlichen und werden regelmäßig überarbeitet.

- Mittels Zugangsmanagementverfahren wird sichergestellt, dass Zugangsberechtigungen für Mitarbeitende im Fall von Veränderungen wie zum Beispiel einem Onboarding, geänderten Rollen in der Organisation oder Beendung des Arbeitsverhältnisses erteilt bzw. widerrufen werden.

16. **Reaktion auf Vorfälle**

- Studytube verfügt über ein dokumentiertes Verfahren zur Reaktion auf Informationssicherheitsvorfälle, um sicherzustellen, dass Zuständigkeiten klar festgelegt sind und bei einem Sicherheitsvorfall angemessen gehandelt wird.

- Studytube verfügt über ein dokumentiertes Verfahren zur Meldung von Verletzungen des Schutzes personenbezogener Daten, das gewährleistet, dass die richtigen Personen gemäß Artikel 33 und 34 der DSGVO informiert werden.

17. **Konformität**

- Studytube unterhält ein nach ISO 27001:2017 zertifiziertes Informationssicherheitsmanagementsystem.

- Studytube ist DSGVO-konform.

- Mit allen Unterauftragsverarbeitern wurden Auftragsverarbeitungsverträge abgeschlossen.

- Sofern dies nicht gesetzlich verboten ist, leitet Studytube behördliche Auskunftsersuchen an die betreffenden Kunden weiter, sodass diese selbst entscheiden können, ob sie die angeforderten Informationen verfügbar machen oder Einspruch gegen das Ersuchen erheben.

STUDYTUBE

Designed with **your future** in mind.

www.studytube.de

Studytube DACH GmbH

Oranienburger Strasse 27

10117 Berlin

sales@studytube.de

Büro: +49 30 30806704

Registernummer: 180915B