Anlage 1 – Technische und organisatorische Maßnahmen

Abschnitt A

Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

1. “*um” - The unbelievable Machine Company GmbH
   Hosting der bettermarks-Server
   10623 Berlin, Grolmanstr. 40

2. “commehr” - Commehr GmbH
   IT-Dienstleister, Wartung der Geräte im bettermarks-Büro
   10777 Berlin, Nürnberger Str. 38

3. “Sendinblue“ GmbH
   Versand von E-Mails an Lehrer (Registrierung, Informationen)
   10179 Berlin, Köpenicker Straße 126

4. “visual4“ GmbH
   IT-Dienstleister, Betrieb des CRM-Systems (keinerlei Daten von Schülern)
   70199 Stuttgart, Schreiberstr. 27

5. Nur wenn bettermarks *nicht* an ein externes Identitätsmanagementsystem (IDM, sog. ID-Broker) angekoppelt wird, werden bei der Nutzung des Systems identifizierenden Informationen (nur von Lehrkräften, nicht von Lernenden) beim folgenden Dienstleister verarbeitet. Somit ist er nur in diesem Falle als Unterverarbeiter zu betrachten. Und nur in diesem Falle können unter Umständen Daten von Lehrkräften in die USA übertragen werden. Details dazu finden sich in der beiliegenden „Datenschutzfolgenabschätzung Cloudflare“.

   “Cloudflare“ GmbH
   IT-Sicherheits-Dienstleister, Schutz der bettermarks Plattform
   80331 München, Rosental 7

Abschnitt B

Vom Auftragsverarbeiter implementierte technische und organisatorische Maßnahmen, insbesondere Art. 28 Abs. 3 Satz 2 lit. c und e DSGVO

Der Auftragsverarbeiter sichert zu, folgende technische und organisatorische Maßnahmen getroffen zu haben:

Maßnahmen zur Sicherstellung der Verfügbarkeit

1 SCHUTZ VOR ÜBERLASTUNG

1.1 Die Zahl der Zugriffe / Abrufe durch Nutzer war zentrale Bezugsgröße bei der Entwicklung der Anwendung.

- Mittels Belastungstest wurde das Verhältnis zwischen der Zahl der aktiven Nutzer und der benötigten Hardware gemessen. Diese Lasttests werden regelmäßig ausgeführt, um eventuelle Änderungen frühzeitig zu erfassen (Änderungen an der Applikation können sich auf die benötigten Ressourcen auswirken).

1.2 Die Systeme und die Hardware wurden so ausgewählt, dass alle Systeme auch großer Last Stand halten.

- Die Kapazität der Systeme ist so bemessen, dass das Doppelte der täglich gemessenen Spitzenbelastung verkraftet werden kann.

1.3 Die Zahl der Nutzer, der verursachte Netzwerkverkehr und die Auswirkungen auf die Systeme werden fortlaufend und automatisch überwacht (Speicher- Cache- und CPU-Auslastung, sowie die Zahl der laufenden Zugriffe/ Prozesse).

- Mittels Nagios, statsd, graphite, ELK werden entsprechende Werte erfasst und überwacht (Logins/Minute, Beendete Übungsserien / Minute). Zusätzlich werden Informationen über den Zustand der Soft- und Hardware der Systeme gesammelt (Betriebssystem, Hardware).

1.4 Wenn eine Überlastung festgestellt wird, können zusätzliche Kapazitäten zugeschaltet werden.

- Es sind Warnschwellen für Nutzung, Auslastung, sowie Hard- und Software definiert. Bei einer Überschreitung werden Alarme ausgelöst.
- Im Bedarfsfall können zusätzliche Maschinen&Kapazitäten zugeschaltet / hochgefahren werden.

2 AUFRECHTERHALTUNG DES BETRIEBES

2.1 Redundante Systeme können praktisch sofort bereitgestellt werden ('Warm Standby'):

- Alle Hardwarekomponenten sind redundant ausgelegt:
    - Hosting in einem zertifizierten, hochverfügbaren “tier-4 data-center” (die höchste Verfügbarkeitsklasse)
    - Internetanbindung, Stromversorgung, Netzwerkkomponenten, Firewalls, Load-balancers – all diese Komponenten sind redundant ausgelegt.
    - Die Server-Hardware, auf denen bettermarks im Rechenzentrum läuft, sind ebenfalls redundant ausgelegt (RAID-5, Stromversorgung, Netzwerkkomponenten).
- Alle virtuellen Maschinen und Dienste der Produktionsumgebung von bettermarks sind redundant ausgelegt.
    - Die redundanten virtuellen Maschinen laufen auf unterschiedlichen Maschinen.
- Es werden geclusterte Datenbanksysteme mit automatisher Ausfallsicherung (Autofailover) eingesetzt.

2.2 Es wird regelmäßig ein Datenwiederherstellungstest mit einem RTO (Wiederherstellungszeitziel) von weniger als 24 Stunden durchgeführt.

- Jedes Wochenende wird automatisch auf einem Testsystem auf Grundlage von anonymisierten Datenbankbackups ein Datenwiederherstellungstest durchgeführt.

3 DESIGN

3.1 Während der Design-Phase der Systeme wurden die Abhängigkeiten der einzelnen Komponenten betrachtet und die Auswirkungen von Ausfällen einzelner Teilsysteme minimiert.

- Abhängigkeiten von externen Systemen werden überwacht und im Falle eines Problems werden Alarme ausgelöst.

- Die Aufrufe externer Systeme (Schulcloud etc.) erfolgen wenn möglich durch resiliente Softwarepraktiken, so dass die bettermarks-eigenen Systeme durch externe Ausfälle nicht in Mitleidenschaft gezogen werden.

4 MONITORING

4.1 Die Verfügbarkeit und die Nutzung werden fortlaufend überwacht.

- Die Erreichbarkeit und Verfügbarkeit von bettermarks wird automatisch in 5-Minuten-Intervallen von verschiedenen Orten auf der Welt geprüft.

- Intern werden alle relevanten Teilsysteme fortlaufend auf Verfügbarkeit geprüft.

4.2 Bei durch das Monitoring entdeckten Problemen beginnt ein strukturierter Benachrichtigungs- und Reparaturprozess.

- Je nach Schweregrad eines Problems werden E-Mails und / oder SMS an einen für den Betrieb verantwortlichen Personenkreis versandt.

- In gravierenden Fällen wird ein sogenannter Betriebsvorfall („Incident“) ausgelöst. Die Regeln für das Auslösen eines „Incidents“ stellen sicher, **dass**

das Problem zügig, effizient und mit allen benötigten Ressourcen behoben werden kann.

5 TESTEN

5.1 Verfügbarkeit und Ausfallsicherheit werden regelmäßig getestet.

- Die redundant ausgelegten Systeme werden regelmäßig ausgeschaltet bzw. heruntergefahren um die Auswirkungen auf die Leistungsfähigkeit des Systems zu messen.

- Die jeweils aktive Datenbank wird regelmäßig ausgeschaltet bzw. heruntergefahren, um das reibungslose Einspringen der Failover-Datenbank zu testen.

5.2 Bettermarks führt proaktiv Leistungstests durch, um Architekturänderungen oder Änderungen im Nutzungsverhalten zu prüfen.

- In regelmäßigen Abständen wird ein synthetischer Belastungstest ausgeführt, welcher eine hohe parallele Anzahl der typischsten Nutzungsvorgänge simuliert (Login/Übungsserie starten / beenden).

6 SOFTWARE

6.1 Sicherheitspatches, Updates der Firmware und Software und Erneuerung von Zertifikaten werden regelmäßig eingespielt.

- Betriebssystem und Softwarekomponenten werden fortlaufend – aber mindestens ein Mal im Jahr aktualisiert.

- Die Gültigkeit der Zertifikate wird überwacht.

6.2 Dringende Sicherheitspatches werden sofort installiert.

- Durch die Automatisierung der Installation der Systeme wurden in der Vergangenheit diese kritischen Sicherheitspatches stets in weniger als

sechs Stunden (nach zur Verfügung stehen) zum Produktionssystem hinzugefügt.

7 BEDROHUNGEN

7.1 Die verantwortlichen Mitarbeiterinnen und Mitarbeiter sind sich der Bedrohungen der Verfügbarkeit bewusst (DoS).

- Ein diesbezügliches “Sicherheitstraining” findet 1x im Jahr statt.
- Im Rahmen der täglichen Team-Besprechung werden auf Grundlage von speziellen Auswertungen auffällige Nutzungsmuster besprochen.

7.2 Durch Monitoring etc. waren wir in der Vergangenheit stets in der Lage, eine Nichtverfügbarkeit innerhalb weniger Minuten festzustellen und Gegenmaßnahmen einzuleiten.

- Es findet ein Monitoring der Zahl der Anfragen und des übertragenen Datenvolumens statt.

7.3 Es gibt einen mehrstufigen aktiven Schutz gegen (D)DoS-Attacken.

- Alle Zugriffe auf bettermarks erfolgen über den Sicherheits-Dienstleister Cloudflare. Angriffe können durch zahlreiche automatisch und manuell ausgelöste Abwehrmethoden (dynamic firewall rules, rate-limiting, Web Application Firewall, ..) bewältigt werden.
- Die Firewall (Fortigate 1500D) und der Loadbalancer (F5) bieten einen aktiven Schutz gegen DoS-Attacken im Rechenzentrum in Berlin.
- Auf Applikations-Ebene gibt es Möglichkeiten, um einzelne bösartige Nutzer auszusperren.

Maßnahmen zur Sicherstellung der Integrität

1 BACKUP

1.1 Ein Backup erfolgt täglich.

- Ein automatisierter Auftrag sichert die Datenbanken einmal am Tag vollständig.
- Die Backups der letzten 11 Tage werden gespeichert.

1.2 Das maximale Alter der geretteten Daten im Falle einer Katastrophen- bzw. Notfallwiederherstellung (Recovery Point Objective) beträgt 24 Stunden.

1.3 Ein Wiederherstellungstest wird regelmäßig durchgeführt.

2 ANWENDUNGSKONTROLLE

2.1 Überprüfung von Eingaben und Anfragen

- Die Anwendung prüft Eingaben durch Syntaxprüfung und Prüfung auf Pflichtfelder.
- Die Web Application Firewall von Cloudflare prüft Anfragen auf OWASP Top 10 sowie andere bekannte Angriffsmuster und ergreift automatisch Gegenmaßnahmen.
- Die Bedrohungserkennung und -behebung wird permanent aktualisiert.

3 BEWEISBARKEIT

3.1 Login–Aktivität von Nutzern und Änderungen an personenbezogenen Daten werden geloggt:

- Login bei bettermarks,
- SSH Login
- Datenbank Login

3.2 Das Logging wird auf unübliche Muster hin (Frequenz, Ursprungsort etc.) überprüft.

- Logins werden überwacht und unübliche Vorgänge lösen Alarme aus

4 RÜCKVERFOLGBARKEIT

4.1 Es ist rückverfolgbar, welche Teile / Konfigurationseinstellungen von bettermarks wann geändert wurden

- Änderungen an den Serverbetriebssystemen werden automatisch angewandt und werden historisiert und sind damit rückverfolgbar.
- Änderungen an der bettermarks-Anwendung werden durch automatische Deployment-Tools vorgenommen (ansible/Jenkins). Dies ist rückverfolgbar und historisiert.
- Auch Änderungen an Web- oder Datenbankservern werden automatisch durchgeführt und sind rückverfolgbar sowie historisiert.
- Änderungen am Produktivsystem, die im Ausnahmefall nicht automatisiert angewandt werden (zum Beispiel im Notfall als Teil eines Incidents), müssen dokumentiert werden und sind nachträglich der Automatisierung hinzuzufügen.

4.2 Es ist möglich, Änderungen rückgängig zu machen

- Da die Änderungen automatisch auf die Server aufgespielt werden und historisiert sind, ist es möglich, auf den Änderungsstand einer älteren Version zu wechseln.

4.3 Nicht personengebundene System- bzw. Admin-accounts (webadmin) sind (indirekt) rückverfolgbar zur nutzenden Person.

- SSH and SUDO – Aktivitäten werden geloggt und können Personen zugeordnet werden.

4.4 Zugriff auf die Serversysteme von bettermarks ist rollenbasiert.

- Für den rollenbasierten Zugriff wird LDAP genutzt.

4.5 Zugriff mit Root-Zugängen wird geloggt und ist reguliert (explicit notification).

- SSH and SUDO-Aktiväten werden geloggt.

5 INTEGRITÄT

5.1 Patches und Firmware- bzw. Softwareupdates werden nach Veröffentlichung schnellstmöglich eingespielt (weitestgehend automatisiert).

- Mindestens ein Mal im Jahr wird das Betriebssystem (und die wesentlichen Komponenten) via automatischer Provisionierungs-Systeme aktualisiert.

Maßnahmen zur Sicherstellung der Vertraulichkeit

1 LEBENSZYKLUS DER DATEN

1.1 Die gesetzlichen Aufbewahrungsfristen für personenbezogene Daten, Logging, Lernerfolge usw. werden eingehalten

- Die Loggingdaten (IP-Adressen zur Abwehr von Gefahren wie DoS-Attacken) werden 7 Tage lang aufbewahrt und dann automatisch gelöscht.

1.2 Wenn ein Nutzer ein volles Schuljahr lang keine Aktivität gezeigt hat (kein Login, keine gestarteten oder beendeten Übungsserien), so werden seine personenbezogenen Daten unwiederbringlich gelöscht.

- Personenbezogene Daten können gelöscht, gesperrt oder korrigiert werden. Zum Beispiel auf Antrag der betroffenen Person bzw. verantwortlichen Organisationen oder nach Ablauf der Aufbewahrungsfrist.
- Es können jederzeit Skripte ausgeführt werden, um alle zu einem Benutzerkonto gespeicherten personenbezogenen Daten automatisch und vollständig und unwiederbringlich zu löschen. Die Aktivitätsdaten sind danach wirksam anonymisiert
- Diese Skripte werden außerdem in regelmäßigen Abständen ausgeführt (Löschung aller Benutzerkonten ohne Aktivität am Ende eines Schuljahres)

2 LOGISCHER ZUGRIFF

2.1 Folgende Richtlinien sind für den logischen Zugriff implementiert:

- Der Zugriff auf Ressourcen im Berliner Rechenzentrum wird über ein zentrales LDAP-System gesteuert
- Benutzer sind einer Organisationseinheit zugeordnet
- Organisationseinheiten werden Berechtigungen für den Zugriff auf Ressourcen erteilt.

2.2 Zusätzliche Authentifizierung

- Der Zugriff auf die Produktionsumgebung im Berliner Rechenzentrum ist nur über VPN möglich

2.3 Die Konten können Personen zugeordnet werden

- Alle Mitarbeiterinnen und Mitarbeiter haben persönliche Konten, um auf die Anlagen im Rechenzentrum zuzugreifen

- Es ist den Mitarbeiterinnen und Mitarbeitern nicht gestattet, technische Konten für den Zugriff auf Rechenzentrumsressourcen zu verwenden

2.4 Regelmäßige Überprüfung der aktiven Konten

- In der Offboarding-Richtlinie ist fest gelegt, dass Konten deaktiviert werden müssen, wenn eine Mitarbeiterin oder ein Mitarbeiter das Unternehmen verlässt
- Regelmäßig wird eine Liste aller nicht aktiven Konten erstellt und überprüft
- Einmal im Jahr werden alle Konten manuell gegenüber aktiven Mitarbeitern überprüft

3 TRENNUNG DER SYSTEME

3.1 Entwicklungs-, Test-, Abnahme- und Produktionsumgebung sind streng getrennt.

- Die virtuellen Maschinen der Umgebungen befinden sich in separaten Subnetzen.
- Die Hosts, aus denen sich die Produktionsumgebung zusammensetzt, hosten keine virtuellen Maschinen aus Nicht-Produktionsumgebungen.

3.2 Produktionsdaten (Benutzernamen, Passwörter, etc.) und persönliche Daten werden nicht in Entwicklungs- und Testumgebungen verwendet.

- Ein automatisches Anonymisierungsskript anonymisiert die Produktionsdaten nach dem Import in Nicht-Produktionsdatenbanken.

3.3 Testdaten sind stets anonym.

3.4 Der Zugriff auf Produktionsumgebungen im Berliner Rechenzentrum wird verwaltet und regelmäßig überprüft.

- Der Zugriff auf die Produktionsumgebung im Berliner Rechenzentrum ist stets nur über VPN möglich.
- Dies wird protokolliert und es gibt Warnmeldungen, um Zugriffsversuche zu identifizieren und zu melden.

4 DATENTRANSFER UND PHYSISCHE SPEICHERUNG

4.1 Verschlüsselung beim Datentransfer

- Der gesamte externe Datenverkehr erfolgt über TLS 1.2 oder höher.
- Der Endpunkt für die benutzerseitigen Zertifikate liegt bei Cloudflare

4.2 Verschlüsselung bei physischer Speicherung.

- Passwörter werden mit SHA256 verschlüsselt.
- Die Datenbanksicherungen werden mit openSSL/AES verschlüsselt.

5 LOGGING

5.1 Der Zugriff auf die bettermarks-Anwendung und die Änderung persönlicher Daten werden protokolliert.

5.2 Die Protokollierung ist nur autorisierten Personen zugänglich und der Zugriff darauf wird wiederum separat protokolliert.

6 TESTS

6.1 Es wurde eine Risiko- / Gefahrenanalyse an der Anwendung durchgeführt.

6.2 Die Anwendung wurde nach Richtlinien geprüft.

- Ein externer Partner führte einen Sicherheitstest durch (IBM app scan) im Jan. 2016.

- Ein kritisches Problem auf Seiten von bettermarks wurde identifiziert und behoben.

7 BEDROHUNGEN

7.1 Die Mitarbeiterinnen und Mitarbeiter sind sich möglicher Bedrohungen bewusst, die zu Datenlecks führen, wissen, wie mit personenbezogenen Daten umzugehen ist und wissen, wo sie Datenlecks in dem Unternehmen melden müssen.

- Mindestens einmal im Jahr findet eine Datenschutzschulung statt.