Baden-Württemberg
DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT

LfDI Baden-Württemberg · Postfach 10 29 32 · 70025 Stuttgart

Per E-Mail

[redacted]

Datum 17. Juni 2020
Durchwahl 0711/615541-0
Aktenzeichen 0221.4-16/15
(Bitte bei Antwort angeben)

Informationsfreiheit: Antrag vom 18. Mai 2020 (FragdenStaat.de #185680, „Analyse zu Threema sowie Moodle / BigBlueButton“)

Sehr geehrter [redacted]

vielen Dank für Ihre Anfrage zu den unserer Pressemitteilung vom 29. April 2020 zugrunde liegenden Analysen der Dienste Threema, Moodle/Big Blue Button und Zoom. Ihre Anfrage ist bei uns am 18. Mai 2020 eingegangen.

Unsere Aussagen zu Threema Work beruhen auf einer Überprüfung der öffentlich auf der Homepage https://threema.ch/de/ zugänglichen Informationen. Wir konnten in diesen Informationen keine gravierenden datenschutzrechtlich relevanten Probleme erkennen.

Hinsichtlich WhatsApp verweisen wir auf unsere Informationen unter

- https://www.baden-wuerttemberg.datenschutz.de/aktuelle-meldungen-alle/ und
- https://www.baden-wuerttemberg.datenschutz.de/duerfen-lehrer-whatsapp-benutzen/.

Unsere Aussage zu Moodle bezieht sich auf die Konfiguration, die bei Belwü (dem Landeshochschulnetz Baden-Württemberg) gewählt wurde. Diese Konfiguration war

bis vor kurzem öffentlich unter https://lehrerfortbildung-bw.de/fb_regional/lfbstandorte/files/moodleV3x/2020-04-08-MoodleV3x-Dokumentation.pdf zugänglich. In unseren Akten findet sich keine Version dieses Dokuments. Bei Durchsicht dieses Dokuments (zu einem Zeitpunkt, bei welchem das Dokument online stand) konnten wir keine gravierenden datenschutzrechtlich relevanten Probleme erkennen. In dieser Konfiguration bietet das Kultusministerien über den Dienstleister Belwü den Schulen in Baden-Württemberg Moodle an.

Auch bei Open-Source-Programmen (z.B. Moodle, BigBlueButton) muss bei der Installation untersucht werden, ob Datenabflüsse an Dritte erfolgen und Konfigurationseinstellungen den datenschutzgerechten Betrieb gewährleisten. Bei Moodle sehen wir dies durch die oben genannte Konfiguration als gegeben an. BigBlueButton speichert in der Standardversion automatisch Videos. Dies muss mit Hilfe einer entsprechenden Konfiguration (disableRecordingDefault=true in der Konfigurationsdatei bigbluebutton.properties) zentral vom Administrator des Systems ausgeschaltet werden. In der Version, wie sie vom Kultusministerium betrieben wird, wurde diese Einstellung vorgenommen, wie uns mündlich und unter Hinweis auf das verwendete Code-Repository unter https://codeberg.org/DigitalSouveraeneSchule/ mitgeteilt wurde. Eine Prüfung des Codes hat ergeben, dass diese Einstellung gesetzt wird, vgl. https://codeberg.org/DigitalSouveraeneSchule/bbb/src/branch/master/roles/bbbcontainer/tasks/main.yml#L136 ff (zuletzt geprüft bei Commit 9c8b4f65378a9b83fa96a035695841a6f409d81b). Auch hier sehen wir deswegen keine datenschutzrechtlichen Bedenken.

Datenabflüsse an Dritte können wir sowohl bei Moodle als auch bei BigBlueButton bei den oben genannten Voraussetzungen nicht erkennen. Diese liegen ebenso wie die Verfügbarkeit unter Kontrolle des Landes. Unabhängig hiervon empfehlen wir zur Verwendung von Browser basierten Anwendungen unter Verwendung eines datenschutzfreundlichen Browsers.

Die unter https://www.baden-wuerttemberg.datenschutz.de/lfdi-gute-entscheidung-fuer-threema-schulen-brauchen-mehr-orientierung/ genannten Kritikpunkte an Zoom werden dort begründet. Aufgrund der besonderen Corona-Situation wurden die Analysen oftmals mündlich besprochen. In Notizen festgehalten wurden folgende Erkenntnisse:

Zusammenfassung

Zoom ist eine Software, die in den letzten Wochen und Monaten durch eine Reihe schwerer Sicherheits- und Datenschutz-Probleme aufgefallen ist. Insbesondere die Desktop-Clients – zu deren Download und Installation der Hersteller die Nutzer permanent drängt – hatten und haben schwere Sicherheitsmängel. So werden veraltete Software-Bibliotheken mit längst geschlossenen Sicherheitslücken genutzt und die Software verwendet sicherheitskritische Konstruktionen. Aufgrund der vorhandenen Sicherheitslücken und die teilweise tiefe Integration ins System sollten die Desktop-Versionen auf keinen Fall genutzt werden. Auch wenn einige sehr schwer wiegenden Sicherheitslücken, bei denen Angreifer das System der Betroffenen übernehmen konnten, behoben wurden, ist fraglich, ob der Hersteller die Vorgaben aus Artikel 32 Absatz 1 Buchstabe b DS-GVO einhält.

Die Website verwendet ohne ausreichende Rechtsgrundlage Tracking-Dienste. Die vermeintliche Einwilligung ist unwirksam, da bereits zuvor einzelne Tracking-Dienste geladen werden, es keine Möglichkeit zur kompletten Ablehnung gibt, die Betroffenen nicht ausreichend informiert werden und keine datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO) gewählt wurden. Registrierungs-E-Mails enthalten Tracking-Pixel um bereits das Lesen von E-Mails zu protokollieren. Neue Nutzer werden gebeten, die E-Mail-Adressen von Kollegen/Teilnehmern anzugeben. Diese erhalten Einladungs-E-Mails ebenfalls mit Tracking-Pixeln, um bereits das Lesen der Mail zu protokollieren. Es ist unklar, auf welcher Rechtsgrundlage diese Verarbeitung stattfindet.

Ausweislich der Datenschutzerklärung erhebt Zoom auch eindeutige Geräte-IDs wie die „MAC-Adresse, andere Geräte-IDs (UDID)“. Eine Rechtsgrundlage dafür ist nicht ersichtlich. Die unnötige Erhebung von eindeutigen Identifizierungsmerkmalen von Geräten kann einen Verstoß gegen Artikel 5 Absatz 1 Buchstabe c (Datenminimierung) und 32 Absatz 1 Buchstabe a (Pseudonymisierung) DS-GVO darstellen, u.a. da damit pseudonyme Nutzung erschwert und verschiedene Pseudonyme einem physischen Gerät zugeordnet werden können.

Technische Mängel

In der Vergangenheit waren laut diverser Medienberichte vor allem die MacOS-Versionen von Zoom von teilweise schwerwiegenden Sicherheitslücken betroffen, siehe u.a.:

- *https://www.heise.de/mac-and-i/meldung/Zoom-auf-dem-Mac-Sicherheitsluecken-erlauben-Lauschen-und-Root-4695129.html*
- *https://www.heise.de/mac-and-i/meldung/Ungewollte-Kameraaktivierung-Apple-stopft-schwere-Luecke-in-Zoom-mit-Silent-Update-4467716.html*

- *https://www.heise.de/security/meldung/Videokonferenzsoftware-Hacker-verkaufen-angeblich-Exploits-fuer-Zoom-Luecken-4703658.html*
- *https://www.heise.de/security/meldung/Videokonferenz-Software-Ist-Zoom-ein-Sicherheitsalptraum-4695000.html*

Der Sicherheitsforscher Thorsten Schröder hat unter https://dev.io/posts/zoomzoo/ eine Reihe aktueller Mängel der Windows-Version aufgeführt. Die wichtigsten davon sind:

- *Nutzung von veralteten und verwundbaren Libraries wie z.B.*
  - *OpenSSL in der veralteten Version 1.0.2o*
  - *curl 7.36.0 mit einer verwundbaren Version von libssh 2 sowie einer libcurl 7.55.1 mit zahlreichen Sicherheitslücken*
  - *libjpeg-turbo version 2.0.0 (mit Remote Code Execution vulnerability)*
- *Potentielle SQL-Injection (CWE-89)*
- *Ein Software-Bestandteil zur Erzeugung und Versand von Absturzberichten liest die Windows-Registry aus. Eine Rechtsgrundlage für die Erhebung*
- *Potentielle Buffer-Overflows (CWE-120, CWE-676) aufgrund schlechter Programmiertechniken*

Grobanalyse Registrierungsprozess

- *Tracking Website:*
  - *Datenschutzerklärung ist nur mit Akzeptieren von Cookies / Tracking erreichbar*
  - *Es findet Tracking (mit Google Analytics) statt, ohne dass eine Einwiligung des Nutzers eingeholt wird*
  - *Der Cookie-Banner stellt keine nach DS-GVO gültige informierte, freiwillige, aktiv und separat erklärte Einwilligung dar.*
  - *Die Datenschutzerklärung ist an vielen Stellen nur auf Englisch verlinkt, aber auch auf deutsch verfügbar*
  - *Beim Drucken ist die Datenschutzerklärung durch sehr dunklen Hintergrund unleserlich; dies lässt sich nur mit deaktiviertem Hintergrund beim Drucken beheben*

- *Zoom versucht, vom Nutzer mittels Nudging eine Zustimmung dafür zu erhalten, ihm „währenddessen Ressourcen [zu] senden“. Was das sein soll ist nicht ersichtlich.*
- *Die Anmelde-E-Mail enthält einen Tracking-Pixel. Zoom versucht damit, bereits das Lesen der E-Mail zu protokollieren.*
- *Nach dem Anmelden wird der Nutzer gebeten, E-Mail-Adressen von Dritten anzugeben um diese einzuladen. Diese Einlade-Mails enthalten auch Tracking-Pixel.*
- *Zoom drängt den Nutzer permanent, die eigene Desktop-Anwendung herunterzuladen und zu installieren. Diese installiert unter MacOS Kernel-Erweiterungen und ist damit tief im System veranklert; unter Windows nicht geprüft.*
- *Meetings können nicht mit dem Browser angelegt werden, sondern nur mit der Desktop-Software oder Smartphone- und Tablet-App.*

Zoom-Android-App (Version 4.6.20553.0413):

Root-Erkennung implementiert

- *Verwendet Cert-Pinning und Split-APK*
- *Passives Mitlauschen via Wireshark (Registrieren, Einloggen, Video-Konferenz starten / beenden)*
    - *android.clients.google.com (für Push-Nachrichten)*
    - *zoom.us*
    - *xmpp*.zoom.us*
    - *zpns.zoom.us*
    - *async.zoom.us*
    - *xmppapi.zoom.us*
    - *logfiles.zoom.us*
    - *zoomva*.zoom.us*

Zoom-iOS-App (Version 4.6.12):

- *https://apps.apple.com/de/app/zoom-cloud-meetings/id546505307*
- *App prüft auf Jailbreak, Vorhandensein bestimmte Netzwerke (VPN, 172.xx, 192.xx, fe80:xx)*

- *Setup:*
    - *reiner Start und Klick auf "Registrierung", keine weiteren Aktivitäten*
- *Auffälligkeiten:*
    - *keine 3rd-Party Tracker bisher gesehen*
    - *bei Crash erfolgt Abfrage Einwilligung, diese ist nicht vollständig lesbar; Nutzung von https://github.com/kstenerud/KSCrash*

Hostnamen bei Wireshark:

- *a104-125-6-88.deploy.static.akamaitechnologies.com*
- *ec2-3-235-71-132.compute-1.amazonaws.com*
- *zoom.us*
- *zoomdv15zc.zoom.us*
- *zoomny124bcz.zoom.us*

- *JB Erkennung*

Eine weitere Analyse bzgl. Cert-Pinning (iOS und Android) und Split-APK (Android) nötig.

Weiterhin verweisen wir auf unsere Antwort zu Ihrer Anfrage „Internes Gutachten zu Zoom [#185691]“.

Mit freundlichen Grüßen
Im Auftrag
des Landesbeauftragten für den Datenschutz und
die Informationsfreiheit Baden-Württemberg