Datenschutz und Datenverarbeitung

Für die Online-Lehrgang- und Video-Konferenz-Plattform unter https://treff.darc.de sind mehrere Server miteinander verbunden, die einen Betrieb von mehreren Konferenzräumen und mehreren hundert Nutzern gleichzeitig ermöglicht. In diesem Dokument soll ein Überblick der getroffenen Maßnahmen gegeben werden, um die anfallenden Daten zu schützen und wie diese verarbeitet werden.

Allgemeiner Überblick

Wer betreibt https://treff.darc.de?

Die Server wurden zu Beginn der COVID-19-Pandemie vom DARC e.V. Referat für Ausbildung, Jugendarbeit und Weiterbildung (AJW) in Koordination mit dem Vorstand und der Geschäftsstelle angemietet. Ziel war es, die kontaktlose Ausbildung fortzuführen. Die Server werden somit vom DARC e.V. betrieben.

Aus diesem Grund trifft die Datenschutzerklärung von www.darc.de ebenso auf treff.darc.de zu: https://www.darc.de/datenschutzerklaerung/

Für wen ist treff.darc.de gedacht?

Ursprünglich war treff.darc.de zur Fortführung von Ausbildungslehrgängen während der COVID-19 Pandemie erstellt worden. Deshalb fiel die Entscheidung auf das Tool *BigBlueButton*, was für Online-Learning seit mehr als einem Jahrzehnt entwickelt wird. Inzwischen steht der treff.darc.de allen Mitgliedern des DARC e.V. offen, um sich kontaktlos und auf Distanz zu treffen. Obwohl Funkamateure Möglichkeiten zur Kommunikation mit Funk haben, ist dieses Verfahren nicht zuverlässig, aufgrund der offenen Sprache nicht optimal für geschlossene Gruppen oder auch schlicht nicht für alle erreichbar.

Die Moderatoren zu Konferenzräumen können entscheiden, ob sie den Zugang offen oder geschlossen halten wollen. Offene Zugänge ermöglicht die Teilnahme durch Gäste, wie beispielsweise Interessierte oder Lehrgangsteilnehmende, die nicht Mitglied im DARC e.V. sind.

Welches Betriebssystem läuft auf den Servern?

Alle Server laufen mit dem Betriebssystem Linux mit der Distribution Ubuntu. Je nach Funktion und Kompatibilität sind verschiedene Versionen von Ubuntu Linux im Einsatz. Alle Versionen erhalten Sicherheitsupdates von Ubuntu.

Wo stehen die Server?

Die Server sind alle beim deutschen Provider netcup GmbH angemietet. Die Rechenzentren befinden sich in Nürnberg. Es werden virtuelle Maschinen eingesetzt, die in der verwendeten Konfiguration keinen Zugang zu anderen virtuellen Maschinen auf demselben Server ermöglichen.

Wer hat Zugriff auf die Server?

Die Server sind im Auftrag von der Geschäftsführung durch die DARC IT angemietet worden, d.h. die DARC IT hat die Zugangsdaten zum Serververwaltungsportal.

Einen administrativen Zugriff haben mehrere Personen eines Admin-Teams, die allesamt Mitglieder des DARC e.V sind. Sie haben die DARC-Vereinbarung zum Datenschutz bei der Arbeit mit Mitgliedsdaten akzeptiert und unterschrieben.

Welche Software wird eingesetzt?

Es wird diverse quelloffene Software eingesetzt:

- *BigBlueButton* für die Videokonferenz mit den dafür hier nicht weiter aufgelisteten Abhängigkeiten
- *NGinX* als Webserver
- *Scalelite* als Loadbalancer
- *Coturn* als Dienst für WebRTC-Verbindungen hinter NAT
- *Prometheus*, *Alertmanager* und *Grafana* für das Monitoring
- Eine eigens entwickelte Raumverwaltung, die den Bedürfnissen des DARC e.V. entspricht

Die Konfiguration der Server erfolgt mittels Ansible. Eine erste Grundlage erfolgte auf Basis des BigBlueButton-Ansible-Repositories von "ulm-lernt". Inzwischen sind diverse eigene Implementationen für treff.darc.de eingeflossen. Das Repository ist unter https://bitbucket.darc.de/projects/TRF/repos/darc-treff-ansible/browse abgelegt.

Datenübertragung

Über welche Verbindungen kann mit den Servern kommuniziert werden?

Zugriff auf die Server erfolgt ausschließlich über SSL-geschützte Verbindungen. Auch die Kommunikation zwischen den Servern erfolgt über SSL-geschützte Verbindungen. Die Server sind über eine statische IPv4- und IPv6-Adresse erreichbar.

Auf den Servern sind Firewalls installiert, die nur die notwendigen Ports öffnen.

Welche Daten werden mit einem Backup gesichert?

Es wird täglich ein Backup der PostgreSQL-Datenbank mit der Benutzer- und Raumverwaltung durchgeführt. Dieses Backup wird für drei Tage lokal auf dem Server gesichert und gleichzeitig auf die NextCloud des DARC (files.darc.de) in den Bereich des Referat AJW kopiert. Diese Backups werden nach frühestens drei Monaten manuell gelöscht.

Benutzerdaten

Welche Rollen gibt es mit welchen Rechten?

Innerhalb einer laufenden Konferenz gibt es vier Rollen:

- Teilnehmer und Gast
  - Kann das eigene Mikrofon freigeben
  - Kann die eigenen Kamera freigeben
  - Kann den Chat lesen und darin schreiben
  - Kann die geteilten Notizen lesen und verändern
- Moderator
  - Alle Rechte eines Teilnehmers
  - Kann einen Teilnehmer zum Präsentator machen
  - Kann Einstellungen eines Raums verändern
  - Kann Teilnehmer stumm schalten (aber nicht wieder einschalten)
  - Kann Kameras deaktivieren (aber nicht wieder einschalten)
  - Kann, wenn es für den Raum aktiviert wurde, die Aufnahme starten und pausieren
  - Kann Gruppenräume aktivieren
  - Sieht das Lern-Dashboard mit der Beteiligung der einzelnen Teilnehmenden während der Konferenz
  - Kann die Teilnehmer-Liste speichern
  - Kann den Chatverlauf speichern und löschen
  - Kann die geteilten Notizen speichern
- Präsentator
  - Ist eine Rolle, die sowohl auf einen Teilnehmer als auch einen Moderator übertragen werden kann
  - Kann Folien hochladen
  - Kann aus bereits hochgeladenen Folien für die aktuell laufende Konferenz auswählen
  - Kann den eigenen Bildschirm freigeben
  - Kann Umfragen starten

In der Raumverwaltung gibt es fünf verschiedene Rollen:

- Teilnehmer:
  - Jedes DARC-Mitglied
  - Kann den Kalender einsehen
  - Kann an öffentlichen Konferenzen teilnehmen
- Raumersteller:
  - Automatisch alle Personen in gewählten Ämtern im DARC e.V. oder nach administrativ vergebenem Raumersteller-Recht
  - Können Räume erstellen, verwalten und löschen
  - Können Kalendereinträge zu diesen Räumen erstellen, verwalten und löschen
  - Haben Zugriff auf die Aufzeichnungen dieser Räume
- Distriktsvorsitzende:
  - Können alle Räume ihres Distrikts sehen
  - Können an allen Konferenzen ihres Distrikts teilnehmen - analog zur Teilnahme an Versammlungen im Distrikt, wie es in der Satzung festgehalten ist
- Vorstand:
  - Können alle Räume sehen
  - Können an allen Konferenzen teilnehmen - analog zur Teilnahme an Versammlungen des Vereins, wie es in der Satzung festgehalten ist
- Administratoren:
  - Können alle Räume sehen
  - Können an allen Konferenzen teilnehmen - ausschließlich zu administrativen Zwecken
  - Können das Raumersteller-Recht vergeben
  - Sehen alle Kalendereinträge
  - Können *nicht* Aufzeichnungen von Räumen sehen

Wer vergibt die Rechte?

Es existiert kein festes Konzept für die Rechtevergabe, sondern es hat sich ein Best Practice Modus entwickelt.

- Teilnehmer sind alle DARC e.V. Mitglieder, die einen Teilnahme-Link zu einer Konferenz erhalten haben.
- Moderatoren sind diejenigen Mitglieder des DARC e.V., die einen Moderdator-Link zu einer Konferenz erhalten haben. Moderatoren können in einer laufenden Konferenz andere Teilnehmer zu Moderatoren machen.
- Gäste sind alle Personen, die eine Gast-Link zu einer Konferenz erhalten haben. Es wird angezeigt, dass ein Gast-Link verwendet wurde.
- Administratoren sind die Personen, die beim Aufbau von treff.darc.de unterstützt haben und Erfahrung mit der Software mitbrachten.

Welche Daten werden von Benutzern erhoben?

Der Login erfolgt mit der Mitgliedsnummer und dem dafür vergebenen Passwort. Vor dem Betreten eines Raums kann ein selbst gewählter Name vergeben werden oder ein anonymer Zutritt erfolgen. Die Nutzung von Audio- und Videodaten ist freiwillig.

Mitglieder mit Raumersteller-Recht werden in der Datenbank zusammen mit den angelegten Rauminformationen gespeichert.

Wie erfolgt die Überprüfung der Benutzerdaten auf DARC e.V. Mitgliedschaft?

Die Raumverwaltung von treff.darc.de ist an die Mitgliederverwaltung des DARC e.V. gekoppelt. Es findet eine Abfrage zu mydarc.de statt, in der in der Abfrage die Mitgliedsnummer und das Passwort übermittelt wird und in der Antwort Name, Rufzeichen, Ortsverband, Funktion und Mitgliedsstatus zurückgesandt wird.

Diese Informationen werden bei der Erstellung eines Raums in der Datenbank von treff.darc.de zu den Rauminformationen gespeichert.

Absicherungen und Analyse

Malware-Schutz durch Uploads

Innerhalb einer Konferenz können Foliensätze hochgeladen werden. Nur eine begrenzte Anzahl an Dateitypen kann verarbeitet werden, da diese intern mit LibreOffice in ein PDF und danach in eine Vektorgrafik im SVG-Format umgewandelt werden. Es kann die Option gesetzt werden, dass Nutzer die erstellte PDF-Datei herunterladen können. Da diese Datei bereits umgewandelt wurde, sind sämtliche in der Ursprungsdatei vorhandenen Makros, interaktiven Elemente oder Videos deaktiviert worden. Die Gefahr einer Infizierung des Computers des Nutzers durch Malware ist hierbei nahezu ausgeschlossen.

Protokollierung / Logging

Zur Analyse des Betriebs und zur Beantwortung von Support-Fragen, wenn etwas nicht wie gewünscht funktioniert, fallen auf den Servern Logdaten an. Dabei werden die IP-Adresse des Nutzers, und der verwendet Webbrowser übertragen. Zusätzlich wird mitgeloggt, welcher Raum besucht wurde und ob Mikrofon, Kamera oder Bildschirmfreigabe aktiv war.

Die Logdateien werden nach fünf Wochen gelöscht.

Monitoring

Für die Sicherstellung des Betriebs werden zu jeder Zeit Daten erfasst, die eine historische Analyse ermöglichen. Hierzu zählen Auslastungsdaten von CPU, RAM, Festplatte und Netzwerk. Zusätzlich gibt es Werte zu der Anzahl der laufenden Konferenzen pro Server mit der Anzahl der Teilnehmenden und der Status, ob Mikrofon oder Kamera aktiviert sind. Nicht aufgenommen wird in der Historie, wer zu welchem Zeitpunkt in welchem Raum aktiv war. Die historischen Daten werden als Graphen für mindestens zwei Jahre gespeichert.

Bei Ausfall eines Dienstes oder Servers werden die Administratoren per E-Mail benachrichtigt.

Ausfallsicherheit

Die Backend-Server sind so gestaltet, dass bei Ausfall eines Servers der Serververbund weiter läuft. Lediglich die Konferenzen auf dem ausgefallenen Server werden beendet und können über die Raumverwaltung auf einem anderen Backend-Server neu gestaltet werden. Der Loadbalancer wird über den Ausfall eines Servers informiert und verteilt keine neuen Konferenzen auf den defekten Server.

Die Raumverwaltung, der Loadbalancer, das Monitoring und der Server für *coturn* sind aus Kostengründen nicht redundant ausgelegt. Der Frontend-Server befindet sich nicht in einem externen Monitoring. Ein Ausfall wird am ehesten durch eine Mitteilung an die Administratoren durch die Nutzer bekannt.

Backup

Es wird lediglich ein tägliches Backup der Nutzer- und Raumdatenbank angelegt, was extern auf den DARC Filesserver übertragen wird.

Backups von Foliensätzen oder Videoaufzeichnungen finden nicht statt. Sollte das Shared Storage ausfallen oder gelöscht werden, sind diese Daten – sofern nicht von den Raumverwaltern selbstständig durchgeführt – verloren.

Updates

Die Server erhalten automatisch Security Updates für das Ubuntu Linux Betriebssystem. Feature-Updates der Frontend-Software werden in den Wartungsfenstern eingespielt.

Bei akuten Sicherheitsproblemen behält sich das Admin-Team vor, Updates außerhalb der Wartungsfenster zu einem günstigen Zeitpunkt mit wenigen Nutzern einzuspielen.

Aufzeichnungen

BigBlueButton ermöglicht die Aufzeichnung von Konferenzen. Hierzu muss vorab in den Raumeinstellungen "Aufnahme des Raumes erlauben" eingeschaltet werden. Teilnehmende an diesem Raum erhalten nun vor der Teilnahme den Hinweis, dass dieser Raum möglicherweise aufgezeichnet wird und müssen dieses aktiv bestätigen. Tun sie das nicht, nehmen sie ohne Mikrofon und Video als anonymer Benutzer an der Konferenz teil.

Werden alle Konferenzen aufgezeichnet?

Nein. Nur solche Räume in denen die oben genannte Einstellung zur Aufnahme des Raums gesetzt wurde, können aufgezeichnet werden. Zusätzlich muss aktiv von einem Raum-Moderator die Aufnahme gestartet werden. Die laufende Aufnahme wird mittels eines roten, runden Buttons am oberen Bildschirmrand für alle Teilnehmende in einem Raum angezeigt.

Jedoch ist bei BigBlueButton die Aufnahme technisch so gelöst, dass bei Räumen in denen die Aufnahme möglich ist, diese vom Start bis zum Ende auf dem Server aufgezeichnet werden. Mit dem Starten und dem Pausieren einer Aufnahme werden lediglich Marken gesetzt, welches aufgezeichnete Material nach Beenden einer Konferenz in ein Video umgewandelt wird.

Sobald die Aufzeichnung automatisiert an den Marken geschnitten und dem Raumersteller bereitgestellt wurde, werden die Rohdaten vom Server gelöscht.

Was wird aufgezeichnet?

Die Aufzeichnung ist systemweit deaktiviert. Eine Aufzeichnung erfolgt nur, wenn dieses für den Raum aktiviert wurde und die Teilnehmenden darüber informiert wurden.

BigBlueButton zeichnet mehrere Sachen auf, die später zu einem Video zusammengefügt werden:

- Folien
- Chat
- Audio
- Webcams
- Bildschirmfreigaben
- Zeichnungen auf dem Whiteboard
- Umfrageergebnisse

Dadurch, dass alles separat aufgezeichnet wird, können später unterschiedliche Arten von Aufzeichnungen bereit gestellt werden. Für treff.darc.de gibt es zwei Arten von Aufzeichnungen:

- Interaktive Aufzeichnung
- Zusammengesetztes MP4-Video

Wird mein Mikrofon dauerhaft übertragen?

Nein. Dieses war in einer älteren BigBlueButton-Version der Fall. Sprache wurde dauerhaft übertragen und nur auf dem Server stumm geschaltet. In der aktuell eingesetzten Version von BigBlueButton ist dieses nicht mehr der Fall und die Stummschaltung erfolgt am Endgerät des Teilnehmenden.

Wo wird die Aufzeichnung gespeichert?

Während die Aufzeichnung läuft wird diese auf dem Server gespeichert, auf dem die Videokonferenz läuft. Das sind die Server mit der Bezeichnung "alfa.treff.darc.de", "bravo.treff.darc.de" usw.

Nach dem Beenden der Konferenz wird auf diesem Server das Video mit den Schnittmarken erstellt. Die finalen Videodateien werden auf ein Shared Storage in diesem Serververbund kopiert und sind danach aus aus der Raumverwaltung erreichbar. Es erfolgt kein weiteres Backup der Daten.

Wie lange werden die Aufzeichnungen gespeichert?

Die Rohdaten werden nach dem automatisierten Erstellen des Schnitts von den Servern gelöscht.

Die fertig geschnittenen Videos auf dem Shared Storage haben keine Aufbewahrungsfristen. Hier liegt die Verwaltung der Videos bei den Raumbesitzern für ihre eigenen Räume und den Administratoren für serverweiten Zugriff.

Wer hat Zugriff auf die Aufzeichnungen?

Im Prinzip hat jede Person Zugriff, die die URL zu den Aufzeichnungen erhält. Diese setzt sich aus https://treff.darc.de/playback und einem (langen, zufälligen und eindeutigen) Konferenz-Code zusammen. Derzeit ist keine Funktion für einen Zugriffsschutz implementiert.

Die Idee dabei ist es, dass beispielsweise Teilnehmende von Lehrgängen durch die Aufzeichnung den Stoff wiederholen können. Dadurch, dass diese häufig kein Mitglied im DARC sind, erhalten sie keinen Zugang mit der Rolle Teilnehmer, sondern sind nur Gast. Diesen kann aber ebenso der Link zur Aufzeichnung zugesandt werden. Ein Download der MP4-Dateien für das eigene Archiv ist möglich.

Innerhalb der Raumverwaltung ist der Zugriff auf die Aufzeichnungen nur den Raumbesitzern möglich.

Mittels Admin-Zugriff kann technisch bedingt auf alle Aufzeichnungen – auch die Rohdaten – zugegriffen werden.