ZOOM, WEBEX, TEAMS &. CO

DAS DIGITALE GRUPPENTREFFEN - AUSWAHL UND EINSATZ VON KONFERENZSOFTWARES FÜR DIE SELBSTHILFEARBEIT

Wer bin ich überhaupt?

- Jahrgang 1978
- Diplom-Soziologe (Medien- und Kultursoziologie, Anthropologie, Geschlechterforschung, Subkulturen)
- freiberuflicher Dozent für Medienkompetenz, hauptsächlich im NGO-Bereich aktiv
- mehr als 20 Jahre Netzerfahrung, beginnend mit analogen Modems und 286er-Rechnern, Amiga 500 & Co.
- enge Zusammenarbeit mit sozialen Einrichtungen, Wohlfahrtsverbänden, Beratungsstellen
- Schriftsteller, Musiker, Blogger, Gamer. Sonst aber ganz nett.

Inhalt

1. Bestandsaufnahme
2. Anforderungen an eine Softwarelösung
3. Vergleich verschiedener Anbieter
4. Tipps für mehr Sicherheit
5. Rechtliches

Bestandsaufnahme

DATENSCHUTZ

Microsoft Teams, Zoom, WebEx: Berliner Behörde warnt vor gängigen Videosystemen

Nach einer ersten Datenschutzprüfung haben einige Videodienst-Anbieter ihre Angebote nachgebessert. Doch die Berliner Datenschutzbeauftragte sieht immer noch gravierende Mängel.

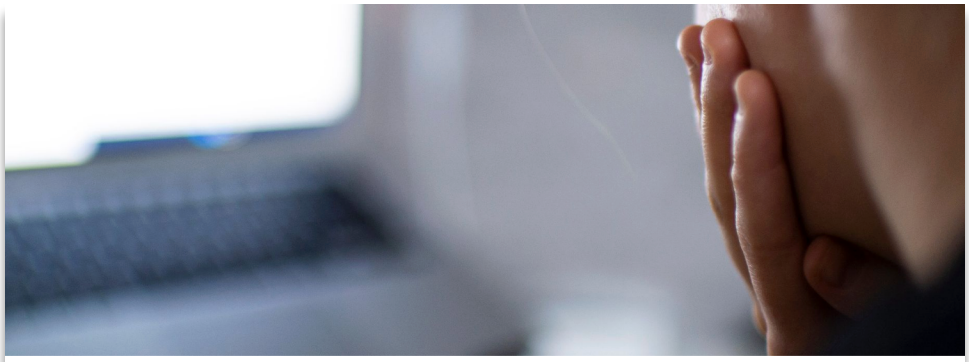
Dietmar Neuerer

18.02.2021 • Update: 19.02.2021 - 08:13 Uhr • 2 Kommentare • 43 x geteilt

Videodienst

Berlins Datenschutzbeauftragte rät von der Nutzung führender Videokonferenzsysteme wie Microsoft Teams ab.
(Foto: dpa)

https://www.handelsblatt.com/politik/deutschland/datenschutz-microsoft-teams-zoom-webex-berliner-behoerde-warnt-vor-gaengigen-videosystemen/26929216.html?ticket=ST-5428670-uSplBxiSc702a7GHc4V1-ap5



20.01.2021, 14:05 Uhr

Unbekannte dringen in Lernchat von Grundschülern ein

Unbekannte haben sich in die Videokonferenz einer Abensberger Grundschulklasse eingewählt und dort beleidigende Videos geteilt. Die Schulleiterin schaltete umgehend die Polizei ein. Man kann sich jedoch vorab auch selbst vor Eindringlingen schützen.

Der Lernchat einer Schule in Abensberg im Kreis Kelheim ist Opfer unbefugter Eindringlinge geworden. Dort teilten diese Videos, in denen Schüler und auch Eltern beleidigt wurden. Die Aktion dauerte laut Polizei mehrere Minuten.

25 Erstklässler betroffen

Wie die Polizei dem BR bestätigte, waren rund 25 Erstklässler zu dem Zeitpunkt des Übergriffs auf der Open-Source-Plattform aktiv. Gegen Mittag bemerkten sowohl Lehrkräfte als auch Eltern, dass Videos im Chat liefen, die nichts mit dem Lernstoff zu tun hatten. Die Schulleiterin verständigte daraufhin die Polizei.

Polizei ermittelt wegen Beleidigung

Vermutlich waren die Täter schlicht an den Link zur Videokonferenz gekommen, wie die Polizei auf BR24-Nachfrage mitteilte. Anfängliche Schilderungen, dass es sich um pornografisches oder rechtsmotiviertes Material handelte, kann die Polizei bisher nicht bestätigen. Die Polizei Kelheim ermittelt vielmehr wegen Beleidigung. An der Grundschule Abensberg wurden die Sicherheitseintstellungen der Lernchats in der Zwischenzeit verschärft.

https://www.br.de/nachrichten/bayern/unbekannte-hacken-homeschooling-lernchat,SMdDLkP

Bestandsaufnahme

- Ausgangslage
- Technologische Gegebenheiten
- Medienkompetenz der Mitglieder
- Datenschutzvorgaben
- besondere Anforderungen

Bestandsaufnahme

Wie sehen Ihre konkreten Anforderungen an eine Konferenzlösung aus?

Soll neben der Möglichkeit, Videochats zu veranstalten, mehr möglich sein? Lehrveranstaltungen? Dateiablage?

Welche Endgeräte werden verwendet? Rechner, mobile?

Wer ist die Zielgruppe? Wie steht es um die Medienkompetenz? Teilnehmerzahlen?

Welche Regelungen/Verbote existieren vom Verband, Bundesland etc.?

Gibt es Besonderheiten, die berücksichtigt werden müssen?

Anforderungen an eine Softwarelösung

Anforderungen

Stabilität

Kontrolle

Datenschutz und -sicherheit

Erweiterbarkeit?

Anforderungen

Stabilität

Beim Einsatz von Lösungen, die auf den Servern der Anbieter laufen, ist die Stabilität primär von der Verfügbarkeit der Server abhängig. »Downtimes« für Wartung etc. können zumeist nicht beeinflusst werden.

Beim Hosten einer eigenen Lösung auf einem eigenen Server können Wartungsarbeiten besser geplant und Lastspitzen vorhergesehen werden. Gleichzeitig liegt der Aufwand für Betrieb und Wartung hier bei der Einrichtung, nicht beim Anbieter der Software.

Wie häufig und für jeweils wie lange soll die Lösung eingesetzt werden?

Anforderungen

Kontrolle

Je nach eingesetzter Lösung gibt es verschiedene Möglichkeiten für Moderation, für das »Abschließen« von Seminarräumen etc. Bei der Auswahl einer Lösung sollte darauf geachtet werden, welche Kontrollfunktionen benötigt werden.

Kontrolle erstreckt sich jedoch auf auf den Umgang mit gespeicherten Daten, abgelegten Dateien etc. Diese Kontrolle ist bei den anbieterseitig gehosteten Lösungen oft nicht gegeben (was zoom beispielsweise mit via Chat herumgeschickten Daten macht, ist nicht wirklich klar).

Anforderungen

Datenschutz und -sicherheit

Hinsichtlich DSGVO-Konformität und Datenhoheit haben die anbieterseitig gehosteten Lösungen Schwächen, da hier oft nicht klar ist, wo genau die Datenverarbeitung stattfindet oder welche Dienstleister involviert sind.

Sofern DSGVO-Konformität erforderlich ist, lässt sich diese am ehesten mit selbstgehosteten Lösungen (z.B. Jitsi, BigBlueButton, NextCloud) erreichen.

Hier sollte genauer überlegt werden, ob die Lösung intern oder extern eingesetzt werden soll (also Kommunikation mit Teammitgliedern oder Klient*innen).

Anforderungen

Datenschutz und -sicherheit

Thema Verschlüsselung: Hier sollte dringend zwischen »Transportverschlüsselung« und echter »Ende-zu-Ende«-Verschlüsselung unterschieden werden.

Erstere sichert nur die Übertragung der Daten gegen Mitlesen, die Daten auf dem Server selbst sind dabei aber nicht wirksam verschlüsselt. »Ende-zu-Ende«-Verschlüsselung bietet derzeit keine der anbieterseitig gehosteten Lösungen.

Besonders der Umgang mit personenbezogenen Daten von z.B. Klient*innen sollte daher eher nicht über derartige Lösungen erfolgen.

Hier haben die selbst gehosteten Lösungen (Jitsi, BigBlueButton, NextCloud) eindeutig einen Vorteile: Hierbei liegen alle Daten auf dem eigenen Server, teils wird auch Ende-zu-Ende-Verschlüsselung unterstützt.

Anforderungen

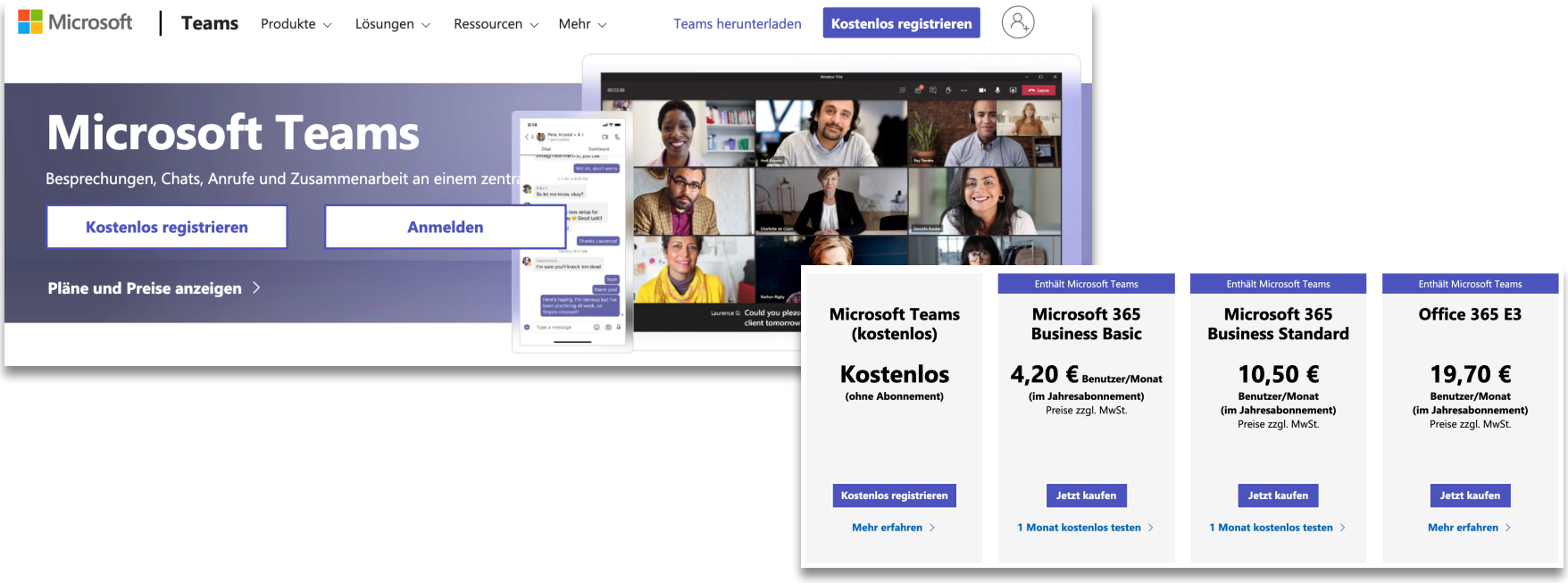
Erweiterbarkeit

Sofern nur eine simple Videochatlösung gesucht ist, ließe sich diese entweder mit günstigen Lösungen wie zoom, Webex & Co. finden (mit den erwähnten Problemen hinsichtlich DSGVO).

Sofern auch Dokumentenmanagement, Forenfunktionen oder andere Anwendungen genutzt werden sollen, fallen oft die günstigen Versionen der Lösungen weg. Alternativ könnte »NextCloud« hier Abhilfe schaffen, die Lösung ist sehr flexibel, was Erweiterungen angeht.

Vergleich verschiedener Anbieter (Auszug)

Microsoft Teams



komplex und kompliziert, kann sehr viel, ist aber unübersichtlich

https://www.microsoft.com/de-de/microsoft-teams/compare-microsoft-teams-options?market=de

Microsoft Teams

Funktionsumfang: sehr hoch

Meetinglänge: 24 Stunden (konstenpflichtige Version)

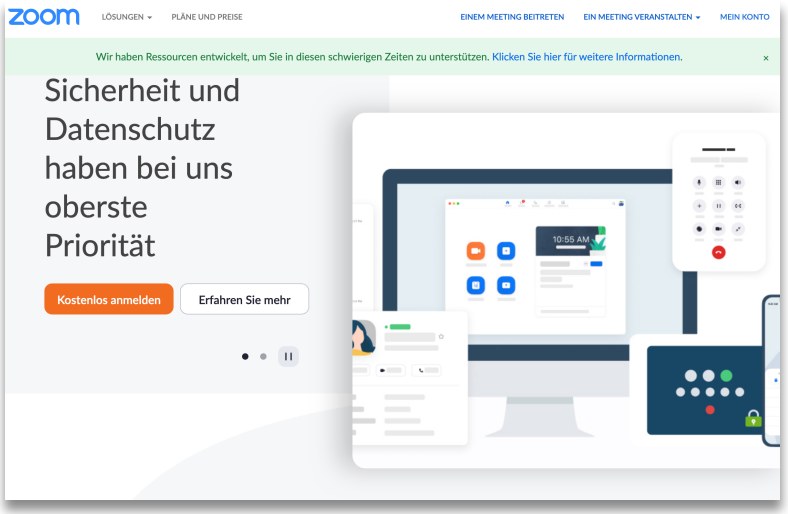
max. Teilnehmerzahl: 300 - 10.000 (je nach Version)

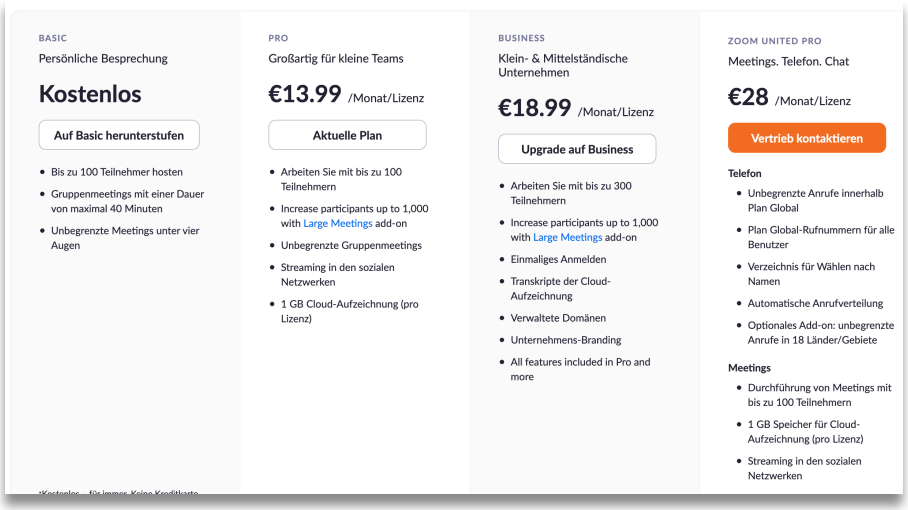
eigenes Hosting möglich: nein

Serverstandort: Datenspeicherung für neue Kunden auch in Deutschland möglich

Im Vergleich zu anderen Lösungen ist »Teams« recht anspruchsvoll in der Bedienung, für wenig medienkompetente Zielgruppe evtl. nicht besonders gut geeignet.

zoom





einfach zu bedienen, zuverlässig, wenig zusätzliche Funktionen

https://zoom.us/pricing

zoom

Funktionsumfang: eher gering

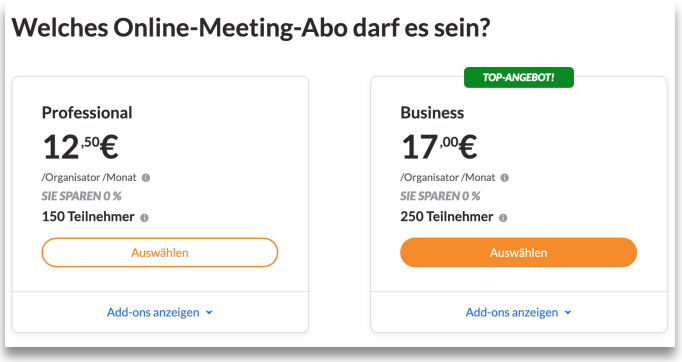
Meetinglänge: ab 40 Minuten (bei kostenloser Version)

max. Teilnehmerzahl: 100-300 (je nach Version)

eigenes Hosting möglich: nein

Serverstandort: Datenfluss während Meetings über deutsche Server möglich, Datenspeicherung im Ruhezustand ungewiss (da wird kein spezieller Standort zugesichert)

GoToMeeting



vom Funktionsumfang im Mittelfeld, Benutzerfreundlichkeit durchschnittlich

https://www.gotomeeting.com/de-de/meeting/preise-gotomeeting-ma

GoToMeeting

Funktionsumfang: mittel-hoch (erweiterbar auf GoToWebinar, kostenpflichtig)

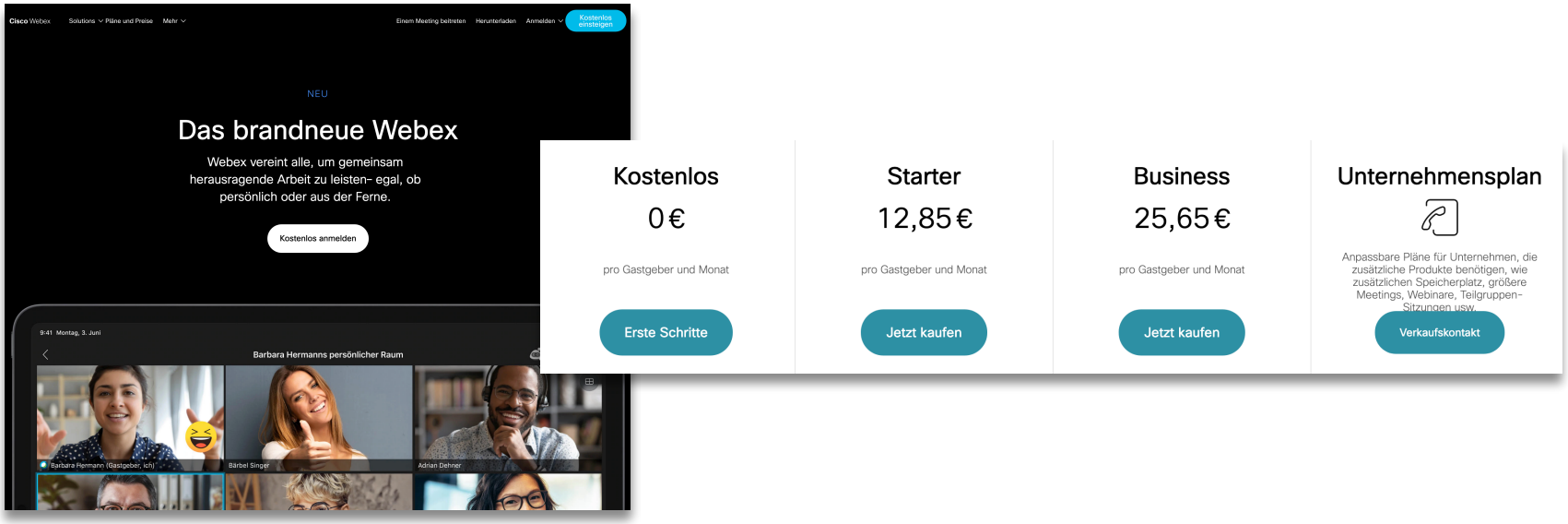
Meetinglänge: laut Website unbegrenzt (bei kostenpflichtiger Version)

max. Teilnehmerzahl: 150-250 (in kostenpflichtiger Version)

eigenes Hosting möglich: nein

Serverstandort: USA (vertraglich DSGVO-konform, aber schlecht überprüfbar)

WebEx



mittlerer Funktionsumfang, recht einfach zu benutzen

https://www.webex.com/de/pricing/index.html

WebEx

Funktionsumfang: mittel-hoch (erweiterbar auf GoToWebinar, kostenpflichtig)

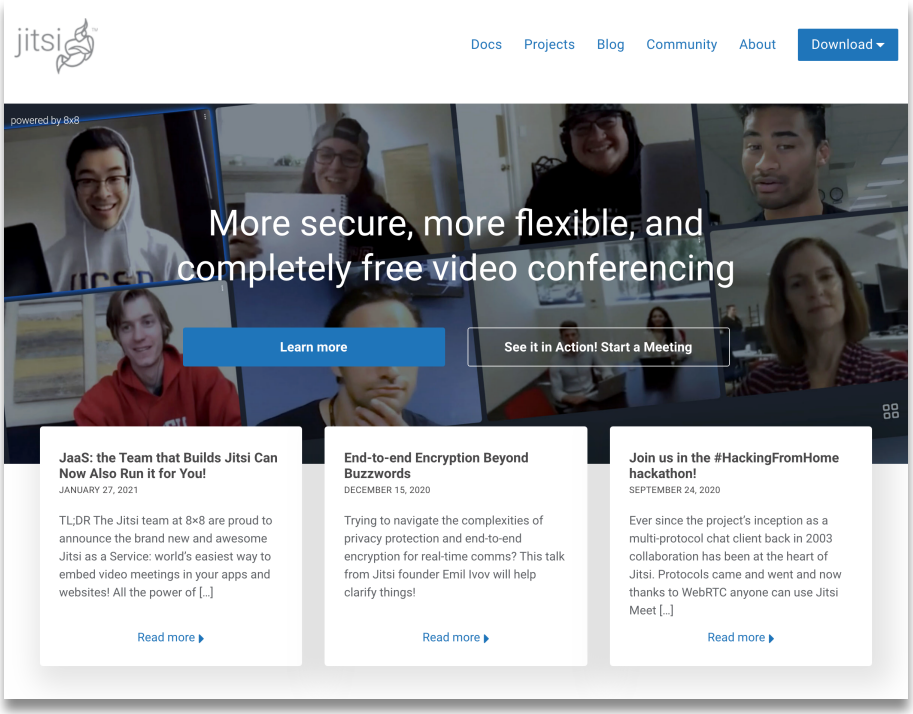
Meetinglänge: laut Website unbegrenzt (bei kostenpflichtiger Version)

max. Teilnehmerzahl: bis 200 (je nach Version, mehr gegen Aufpreis)

eigenes Hosting möglich: nein

Serverstandort: EU ist möglich (Amsterdam), nach Aussage auf der Website werden die Nutzerdaten im geografisch nächstgelegenen Rechenzentrum gespeichert

Jitsi



quelloffen, kostenlos nutzbar (auf fremden Servern) bzw. selbst zu hosten

https://meet.jit.si/

Jitsi

Funktionsumfang: gering-mittel

Meetinglänge:

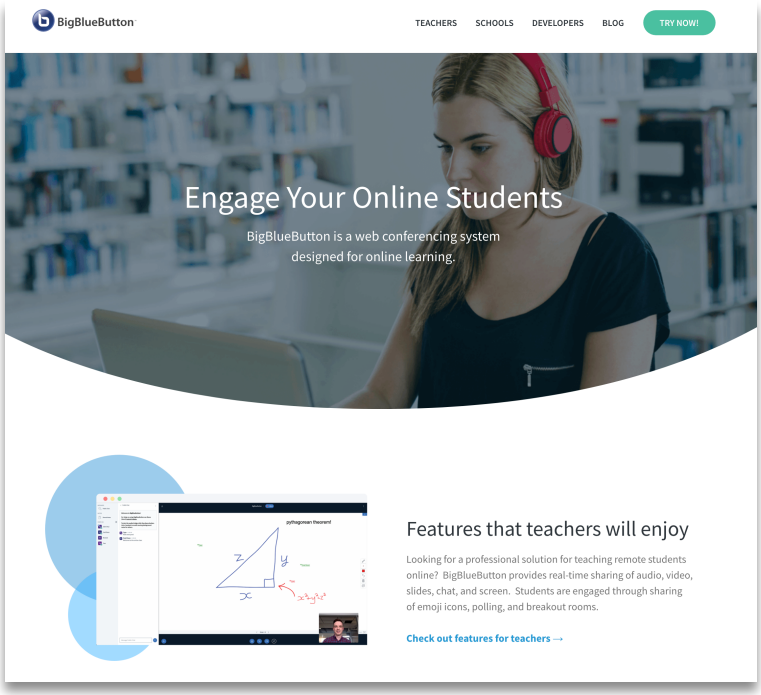
max. Teilnehmerzahl: Chat unbegrenzt, Video 50 (Bandbreite und Server müssen gut ausgestattet sein)

eigenes Hosting möglich: ja

Serverstandort: eigener Server, ansonsten Fremdserver (diese können sich quasi überall befinden)

Jitsi-Server selbst aufsetzen:
https://t3n.de/news/jitsi-meet-server-aufsetzen-1274317/

BigBlueButton



quelloffen, kostenlos nutzbar (auf fremden Servern) bzw. selbst zu hosten

https://bigbluebutton.org/

BigBlueButton

Funktionsumfang: mittel (kann durch Integration in andere CMS erhöht werden)

Meetinglänge: je nach Server 60 min oder länger

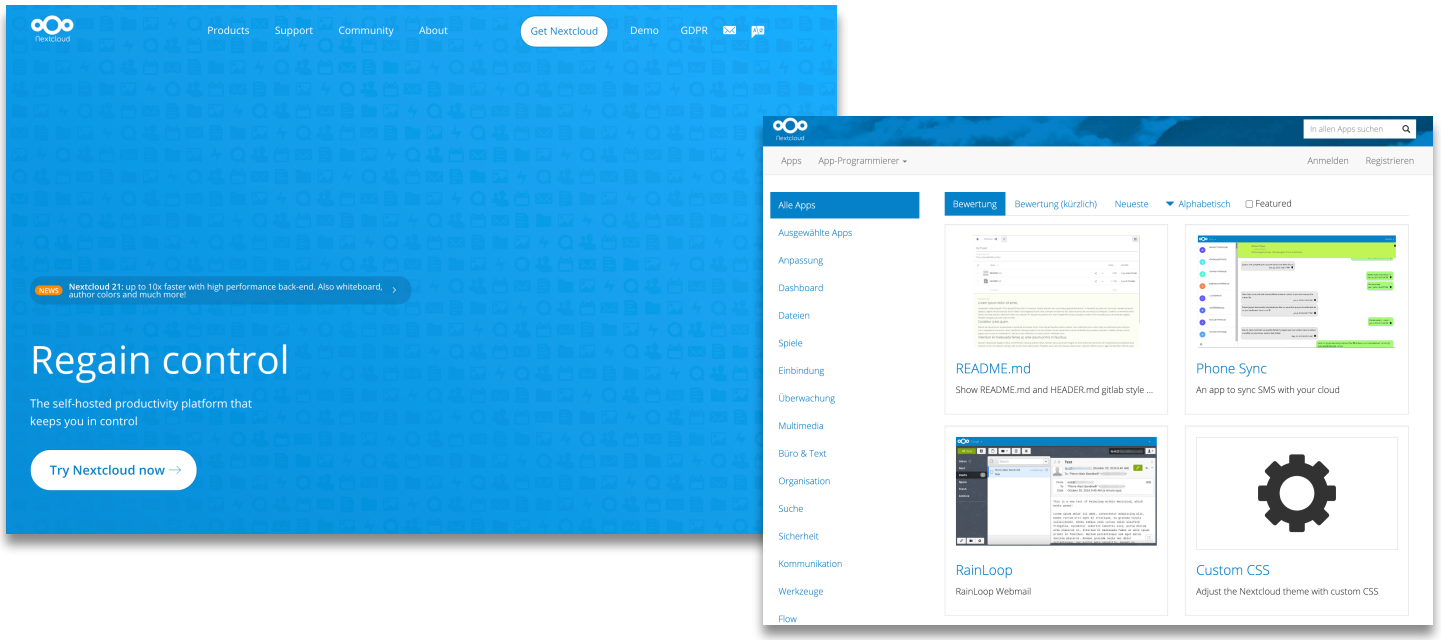
max. Teilnehmerzahl: empfohlen werden max. 100 pro Server

eigenes Hosting möglich: ja

Serverstandort: eigener Server, ansonsten Fremdserver (diese können sich quasi überall befinden)

Beispiel-Dienstleister, der Hosting bieten: https://bbbserver.de/preise/

NextCloud



quelloffen, extrem flexibel, CMS-Funktionen, selbst zu hosten

https://nextcloud.com/

NextCloud

Funktionsumfang: sehr hoch (durch zahlreiche Erweiterungen)

Meetinglänge: unbegrenzt, je nach Konfiguration

max. Teilnehmerzahl: 10-50 TN Video (abhängig von Serverleistung)

eigenes Hosting möglich: ja, für vollständige Datenhoheit empfohlen

Serverstandort: eigener Server, ansonsten Fremdserver möglich

Empfehlung

Aus Sicht der Datenhoheit und der Sicherheit ist eine selbst gehostete Lösung (Jitsi, BBB, NextCloud) zu empfehlen. Noch dazu sind dies OpenSource-Programme, die keine Kosten (außer Wartung) erzeugen.

NextCloud stellt im Vergleich zu den anderen Lösungen, die sich primär auf Konferenzen beschränken, eine voll ausgewachsene Plattform-Lösung dar, die beliebig erweitert werden kann (Foren, Chatrooms, Dateiablage und vieles mehr).

Nachteil der selbst gehosteten Lösungen: ein eigener Server ist sinnvoll, aber Einrichtung, Wartung, Updates etc. müssen selbst sichergestellt werden.

Tipps für mehr Sicherheit

Absichern des Meetings

Nutzen Sie die Möglichkeiten, den Zugang zu Meetings einzugrenzen, um ungebetenen Besuch zu verhindern.

Nutzen Sie die Möglichkeit, Passwörter für den Zugang auszugeben.

Bitte verwenden Sie für jede Sitzung unterschiedliche Zugangsdaten, um das »Hijacken« von Konferenzen zu erschweren.

Passwörter sollten dabei ausreichend komplex sein: Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen, idealerweise zwölf oder mehr Zeichen.

Erstellen Sie Meetings nur mit der Dauer, die benötigt wird und schließen Sie diese danach. Sonst könnten danach eventuell noch Nutzer*innen in den Meetingraum gelangen.

Halten Sie alles aktuell

Sowohl die installierten Versionen der Softwares (z.B. Jitsi, BBB oder NextCloud) als auch die Betriebssysteme von Rechnern und Mobilgeräten sowie verwendete Clients und Browser sollten stets auf dem aktuellen Stand sein.

Nur so lässt sich technisch einwandfreies und vor allem sicheres Funktionieren gewährleisten.

Die Aufgabe, Systeme zu aktualisieren, darf auf keinen Fall auf die leichte Schulter genommen werden. Hierfür sollten Mittel bereitgestellt werden.

Aufzeichnungen

Klären Sie vor Beginn einer Aufzeichnung eines Meetings unbedingt ab, ob die Teilnehmer*innen einverstanden sind. Sowohl Video- als auch Audioaufnahmen dürfen nur mit Einverständnis angefertigt werden.

Achten Sie darauf, Aufzeichnungen möglichst direkt auf einem lokalen Rechner durchzuführen. Bei Aufzeichnungen in der »Cloud« ist oftmals nicht sichergestellt, dass diese DSGVO-konform gespeichert werden.

Für lokale Aufzeichnungen kann alternativ auf das kostenlose Programm »OBS - Open Broadcaster Software« zurückgegriffen werden.

Rechtliches

Bundesländer & Co.

Prüfen Sie vor der Entscheidung für eine Lösung, welche Einstellung der/die Datenschutzbeauftragte Ihres Bundeslandes sowie ggf. Ihr Dachverband zu einzelnen Lösungen hat.

Leider gibt es keine bundeseinheitliche Stellungnahme, lediglich die Behörden der Bundesländer geben Empfehlungen heraus.

In Berlin beispielsweise wird keine der anbieterseitig gehosteten Lösungen empfohlen :)

DSGVO allgemein

Die Datenschutzgrundverordnung stellt Anforderungen an die Speicherung »personenbezogener Daten«.

Auch beim Einsatz von Konferenzlösungen muss dies beachtet werden. Der Serverstandort, das Vorhandensein von Verschlüsselung, DSGVO-konforme AGB und die Verfügbarkeit eines Vertrags zur Auftragsdatenverarbeitung sind nur Beispiele für diese Anforderungen.

Grundsätzlich muss der Serverstandort nicht Deutschland sein, EU wäre ausreichend, selbst Anbieter aus dem Nicht-EU-Ausland unterliegen der DSGVO, hier ist aber oft nicht das nötige Schutzniveau garantiert.

DSGVO allgemein

Beispiel: Eine Einwilligung von Teilnehmer*innen kann für die Teilnahme an einer Konferenz erforderlich sein, sofern diese sich mit privaten E-Mail-Adressen von privaten Geräte aus anmelden.

Die Einwilligung sollte idealerweise schriftlich erfolgen und sollte in jedem Fall nachweisbar sein (siehe Art. 7 DSGVO).

Auftragsdatenverarbeitung

Vor dem Einsatz einer Konferenzlösung sollten Sie unbedingt einen »Vertrag zur Verarbeitung von Datenverarbeitung im Auftrag« schließen.

Dieser ist rechtlich nötig, sobald ein Dienstleister (Anbieter einer Lösung, Serverbetreiber etc.) personenbezogene Daten in Ihrem Auftrag verarbeitet.

Technikgestaltung

Wenn Sie selbst eine Lösung hosten oder per NextCloud eine richtige eigene Plattform anbieten, achten Sie bitte auf die Vorgaben nach Art. 25 DSGVO (»Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen«).

Schützen Sie Ihre Nutzer*innen so gut wie möglich, auch vor deren eigener Naivität :)

Vielen Dank für Ihre Aufmerksamkeit!

Sascha Dinse
Stralauer Allee 17b
10245 Berlin

sascha@sozialvernetzer.de
0175 860 255 7