Selbsthilfe in der Corona-Krise

Erste Empfehlungen für virtuelle Gruppentreffen

Stand: 1. April 2020

Gruppentreffen können momentan nicht stattfinden und viele Selbsthilfeaktive weichen daher auf virtuelle Treffen aus – zumeist auf Videokonferenzen. Für viele Betroffene ist dies ein extrem wichtiger Schritt, der hilft, die momentane, sehr schwierige Zeit zu überbrücken!

Wir möchten Ihnen ein paar erste Tipps für solche virtuellen Treffen geben – weisen aber darauf hin, dass auch wir noch viel zu lernen haben, und daher in den kommenden Wochen immer wieder Updates und Ergänzungen zu diesen Tipps veröffentlichen werden.

Welche Videokonferenz-Anwendungen eignen sich?

Häufig genutzte Anwendungen für Videokonferenzen sind Zoom und Skype. Beide Anwendungen haben Mängel, was den Datenschutz anbelangt.

Als datenschutzfreundlichere Alternative wird Jitsi Meet empfohlen (siehe https://digitalcourage.de/blog/2020/corona-homeoffice-tipps#2).

Jitsi Meet ist kostenfrei und wird direkt im Browser, also ohne Download eines Programms, genutzt. Die Anwendung wird dezentral gehostet: So hat sich bereits jetzt ein großes Netz aus Organisationen, Firmen und Privatpersonen gebildet, die für Jitsi Meet Serverplatz zur Verfügung stellen. Unter anderem kann es auf der Seite meet.golem.de genutzt werden.

Auf der Seite https://www.golem.de/news/videokonferenz-programme-im-test-buero-zu-homeoffice-auf-2003-147206-4.html gibt es einen ausführlichen Überblick über weitere Anwendungen für Videokonferenzen – allerdings nur im Hinblick auf ihre Funktionalität. Datenschutz spielte bei der Bewertung keine Rolle.

Grundsätzlich zu beachten

Egal, welche Anwendung Sie nutzen, sollten die folgenden Fragen im Vorfeld geklärt werden:

Zugang

- Überlegen Sie, wer Zugang zu der Videokonferenz haben soll, und wie dies abgesichert werden kann (z.B. Link / ID nicht veröffentlichen; Weitergabe an Dritte untersagen; bei manchen Anwendungen kann ein Passwort vergeben werden).
- Verfügen alle über die nötigen technischen Voraussetzungen? Sonst empfiehlt es sich, auch eine Beteiligung über das Telefon zu ermöglichen (Das geht in vielen Anwendungen).

Schutz der Vertraulichkeit / Anonymität

- Kenne (und vertraue) ich als einladende Person den anderen, die an dem Treffen teilnehmen sollen?
- Kennen (und vertrauen) sich die anderen Personen untereinander?

Vor allem, wenn dem nicht so ist, muss gemeinsam über die Frage gesprochen und entschieden werden, wie die Anonymität / der Persönlichkeitsschutz der beteiligten Personen gewahrt werden kann.

Aber auch, wenn sich die Personen aus herkömmlichen Gruppentreffen kennen, sollten diese Frage für die digitalen Treffen neu besprochen und hierzu Verabredungen getroffen werden (am besten schriftlich).

Also z.B. miteinander vereinbaren:

- dass niemand Screenshots oder Audioaufnahmen von der Videokonferenz und (ggf.) dem Chatverlauf macht
- dass nichts, was besprochen wird, an andere weitergegeben wird
- dass keine Außenstehenden (z.B. Familienmitglieder) den Bildschirm während der Videokonferenz einsehen können
- dass jede*r für sich prüft, ob er*sie möchte, dass der (vollständige) Name unterhalb des eigenen Bildes eingeblendet wird

Wenn eine „normale“ Gruppe, bei der sich die Teilnehmenden gut kennen, über die Corona-Zeit ihre Treffen in den digitalen Raum verlegt, ist die Wahrung der Vertraulichkeit vermutlich weniger problematisch.

Wenn virtuelle Treffen aber auch für neue Personen offen sein sollen, müssen hier mehr Vorkehrungen getroffen werden. Überlegen Sie sich, wie Sie mit Interessierten vorab ins Gespräch gehen können, um zu prüfen, ob diese mit „guten Absichten“ kommen. Keinesfalls sollten Sie unbekannte Personen – ohne ein vorheriges Gespräch und ohne eine Zusicherung, dass sie an die Vereinbarungen zur Vertraulichkeit halten werden – in eine Videokonferenz lassen. Denn ein Screenshot ist schnell gemacht und im schlechtesten Fall werden dabei zu den Bildern auch noch die vollständigen Namen der Teilnehmenden angezeigt. Ebenso ist es denkbar, dass jemand unbemerkt eine Audioaufnahme des Gesprochenen anfertigt.

Ebenfalls nicht auszuschließen ist, dass jemand zufällig in Ihre Videokonferenz reingerät. Dies ist in den vergangenen Wochen bei Zoom offenbar geschehen, in dem Menschen auf gut Glück eine Zugangs-ID eingetippt hatten. Machen Sie sich daher unbedingt vor der ersten Nutzung gut mit den Einstellungsmöglichkeiten der jeweiligen Videokonferenz-Anwendung vertraut: Damit Sie im Notfall wissen, wie uneingeladene Personen stumm zu schalten oder aus der VK zu entfernen sind. Zusätzlich können Sie sich (bei Zoom) entscheiden, ein Passwort zu vergeben und die Funktion „Nur bestätigte User können teilnehmen“ auszuwählen.

Und auch wenn das jetzt eventuell anders klang: Lassen Sie sich keine Angst machen und probieren Sie es einfach mal aus. Wir wünschen Ihnen viel Spaß und Zufriedenheit mit ihren digitalen Treffen und freuen uns, von Ihren Erfahrungen zu hören.

Wenn Sie Ihre Erfahrungen mitteilen möchten, schreiben Sie gerne eine E-Mail an miriam.walther@nakos.de.