Kurzhinweise zur Absicherung von Videokonferenzen und digitalen Veranstaltungen gegen Störungen (‚Zoom-Bombing')

Fabian Kraetschmer
Referatsleiter IT, Konsistorium
Evangelische Kirche Berlin-Brandenburg-schlesische Oberlausitz

EVANGELISCHE KIRCHE
Berlin-Brandenburg-schlesische Oberlausitz

1. • Wägen Sie ab, wie offen die Veranstaltung sein soll
2. • Machen Sie sich vertraut mit den möglichen Sicherheitseinstellungen des von Ihnen gewählten Produktes
3. • Erkundigen Sie sich ggf. über eine Ihre Veranstaltung betreffende Sicherheit- und Bedrohungslage
4. • Nehmen Sie technisch-organisatorische Hilfe in Anspruch
5. • Aktivieren sie bereits im Vorfeld alle notwendigen und möglichen Sicherheitseinstellunen
6. • Bleiben sie während der Veranstaltung wachsam
7. • Reagieren Sie bei Störungen sofort und sehr deutlich. Seien Sie nicht zurückhaltend beim Entfernen von Teilnehmenden.
8. • Passen Sie das technich-organisatorische Sicherheitskonzept zu folgenden Veranstaltungen ggf. an.

Kurzhinweise zur Absicherung von Videokonferenzen und digitalen Veranstaltungen gegen Störungen (‚Zoom-Bombing')

Einleitung

Digitale Veranstaltungen der Kirche nehmen in Anzahl und inhaltlicher Ausgestaltung stark zu. Die Pandemie sorgt für erhöhte Aufmerksamkeit gegenüber solchen Veranstaltungen. Sie sind einer ungleich höheren Gefährdung für Störungen und Sabotage ausgesetzt, da die Hemmschwelle niedriger ist, die Technik es einfach macht und sich die Täter*innen in einer gewissen, durch das Internet gegebenen, Anonymität wähnen können.

Veranstaltende müssen abwägen zwischen dem möglichst barrierearmen Zugang zur Veranstaltung einerseits und möglichst hoher Sicherheit andererseits.

Barrierearme Zugänge werden u.a. dadurch geschaffen, dass die Zugangsdaten zu einer Videokonferenz öffentlich gemacht und über möglichst viele und unterschiedliche Wege publiziert werden, um möglichst viele Menschen zu erreichen. Veranstaltende können diese Zugangsdaten auf Webseiten, in Print-Publikationen und in diversen sozialen Netzen veröffentlichen. Dies bringt mit sich, dass auch Störer diese Zugangsdaten einfach erhalten und somit zunächst unauffällig an einer Veranstaltung teilnehmen können. Jede Sicherung der Veranstaltung im Sinne des Zurückhaltens der Zugangsdaten erhöht die Zugangsbarrieren. Eine dezidierte Anmeldung der Teilnehmenden oder eine Übermittlung des Zugangskennwortes über zweite Wege tragen zu einer Erhöhung der Zugangsbarriere bei. Für manche Veranstaltungsformate mag eine starke Sicherung zu Lasten der Barrierearmut Sinn haben und möglich sein, für wieder andere trifft das nicht zu. Einzig die Entscheidung gegen partizipative Formate und das Streamen einer Veranstaltung ohne Rückkanal lässt das Risiko einer Störung gegen Null sinken (von den Kommentarspalten unter z.B. YouTube-Videos abgesehen – diese müssen auch beim Streaming von Inhalten überwacht werden). Gerade die partizipativen Elemente (Sprechen, Schreiben, sehen und gesehen werden) machen aber besonders erfolgreiche digitale Veranstaltungsformate aus.

Diese Ausführungen hier beziehen sich auf den Videokonferenzdienst Zoom, vieles wird aber auch auf andere Videokonferenzdienste anwendbar sein.

Technische Hinweise

Folgende technische Einstellungen sollten in Zoom vorgenommen werden, um das Risiko einer Störung zu senken oder um bei auftretender Störung schnell reagieren zu können:

- Aktivieren der Warteraumfreigabe
- Den Teilnehmenden nur mit Vorsicht die Funktionen freigeben:
    - Bildschirm freigeben
    - Chat
    - Sich umbenennen
    - Sich selbst die Stummschaltung aufheben
    - Video starten

Möglicherweise ist es sinnvoll, die Veranstaltung in zwei Break-Out-Räume zu unterteilen und den einen der beiden als ständigen Warteraum, den zweiten als eigentlichen Veranstaltungsraum zu verwenden. Dies verlangt aber nach mehr technischem Verständnis.

Kurzhinweise zur Absicherung von Videokonferenzen und digitalen Veranstaltungen gegen Störungen (‚Zoom-Bombing')

Mögliche Bedrohungsszenarien und was dagegen getan werden kann

Die Erfahrung aus zwei größeren Online-Gottesdiensten zeigen, dass es zu folgenden Störungen kommen kann:

Je nach Veranstaltungsformat können Störungen unterschiedlicher Art auftreten:

- Per Video (Einblendung von unerwünschtem Inhalt oder unerwünschtes Verhalten)
- Audio (Einspielen von unerwünschtem Inhalt oder Sprechen von ungewünschten Inhalten)
- Bildschirmteilung unerwünschter Inhalte
- per Chat (Schreiben unerwünschter Inhalte, Teilen von unerwünschten Dateien)
- per Einblendung störender Profilfotos

Durch Verwenden der Warteraumfreigabe ist zumindest sichergestellt, dass Störer nicht unkontrolliert in die Veranstaltung stürmen. Der Videoraum sollte bereits 20-30min vor Veranstaltungsbeginn geöffnet sein, um die Teilnehmenden nach und nach einzulassen. Beim Betreten der Teilnehmenden des eigentlichen Videoraumes hat es sich als sinnvoll herausgestellt, die Teilnehmenden zu bitten, sich kurz per Video, Audio oder Chat zu melden. Hierdurch kann, genauso wie am Namen des Teilnehmenden recht gut eingeschätzt werden, ob es Störende oder ordentliche Teilnehmende sind.

Auch wenn es der erste Reflex sein mag, ist es unbedingt zu vermeiden, nach Beginn der Veranstaltung alle Beitretende ohne Vorsicht sofort vom Warteraum in das Meeting eintreten zu lassen. Sinnvoll ist es, Teilnehmende aus dem Warteraum in kleinen Schüben eintreten und erstmal das Verhalten durch das technisch/organisatorische Team beobachten zu lassen (Details unten).

Die Erfahrung aus den letzten gestörten Veranstaltungen zeigt, dass Störungen verschiedener Personen gleichzeitig und massiv auftreten. In den vorliegenden Beispielen traten jeweils weit mehr als 10 Störende auf, die mehr oder weniger schnell hintereinander begonnen haben, zu stören. Beim Feststellen einer Störung muss möglichst schnell:

1. Alle wahrnehmbar störenden Teilnehmer entfernt werden (Störung über Ton und Inhaltsfreigabe)
2. Parallel: Eventuell noch vorhandene Rechte für die Teilnehmenden eingeschränkt werden (Recht auf Aufhebung der eigenen Stummschaltung, Recht auf Chat, Recht auf Teilen des Bildschirmes etc.)
3. Alle übrigen störenden Teilnehmer entfernt werden (Störung über Bild oder Chat)
4. Das Meeting gesperrt werden (das bedeutet, dass kein Teilnehmer mehr in den Warteraum kommt. Dies kann später wieder rückgängig gemacht werden)
5. Ggf. per ‚Love-Bombing' in den Chat geschrieben werden, unerwünschte Nachrichten werden so durch das Hineinkopieren z.B. des Vater Unsers für die Teilnehmenden weniger sichtbar, weil sie nach oben geschoben werden

Sobald eine Störung erkannt oder auch nur deutlich vermutet wird, sollte sofort mit den oben beschriebenen Maßnahmen begonnen werden. Je mehr Störer gleichzeitig auftreten, desto schwerer ist es, die Veranstaltung für die Teilnehmenden störungsfrei weiterlaufen zu lassen. Im Zweifel ist es sogar besser, Teilnehmende nur aus Verdacht zu entfernen (und sich hinterher zu entschuldigen), als Störende zu wenig zu entfernen und damit zu riskieren, dass die Teilnehmenden die Störung mitbekommen oder die Veranstaltung sogar abgebrochen werden muss. Bei aktivierter Warteraumfreigabe (dringende Empfehlung!) und bereits entfernten Störenden aus dem Videoraum wird es vorkommen, dass weitere Störer in den Warteraum eintreten. Hier muss durch die Veranstaltende entschieden werden, ob die Veranstaltung schon so weit fortgeschritten ist, dass eine

Teilnahme durch neu hinzukommende ordentliche Teilnehmende nicht mehr sinnvoll erscheint und man die Teilnehmenden nicht mehr aus dem Warteraum einlässt oder ob mutmaßlich ordentliche Teilnehmende doch noch eingelassen werden sollen. Im letzteren Fall hat sich als sinnvoll herausgestellt, dass ein Helfender den Teilnehmenden aus dem Warteraum einlässt und ein anderer Helfender mit der Maus auf dem Entfernen-Knopf einige Minuten wartet, ob von dem gerade eingelassenen Teilnehmenden Störungen ausgehen, um diesen dann sofort entfernen zu können.

Sollte die Situation durch die oben beschriebenen Maßnahmen nicht in den Griff zu bekommen sein, gibt es noch die Möglichkeit, bei Zoom die Funktion ‚Aktivitäten der Teilnehmer aussetzen' zu wählen. Dies bewirkt, das sofort alle Teilnehmende stummgeschaltet, deren Videos und Profilfotos deaktiviert und das Ihnen alle Rechte entzogen werden. Dies ist ein massiver Eingriff in die Veranstaltung und kann nur der letzte Versuch sein. Sobald diese Funktion ausgelöst wurde, fällt es schwerer, zu identifizieren, wer Störender ist und entfernt werden muss und wer ordentlicher Teilnehmender ist. Die Rechte, die nach dem Auslösen wieder den Teilnehmenden zugeteilt werden sollen, müssen manuell zugeteilt werden. Nach dem das getan ist, sollte wieder sehr schnell auf neu aufkommende Störungen reagiert werden.

Ein Szenario ist nur sehr schwer in den Griff zu bekommen:

Alle Störende mischen sich zunächst unauffällig zwischen die ordentlich Teilnehmenden, warten einige Minuten nach Beginn der Veranstaltung und beginnen dann nahezu gleichzeitig mit der Störung. Dies wird in jedem Fall für eine deutliche Beeinträchtigung der Veranstaltung sorgen, ist aber grundsätzlich mit den oben beschriebenen Maßnahmen in den Griff zu bekommen. Sollte sich die Situation nach einem solchen Angriff wieder beruhigt haben, ist es ggf. sinnvoll, die Teilnehmenden zu informieren, Ängste zu nehmen, das Geschehen zu erläutern und erst dann wieder die Veranstaltung fortzusetzen.

Kurzhinweise zur Absicherung von Videokonferenzen und digitalen Veranstaltungen gegen Störungen (‚Zoom-Bombing')

Organisatorische Hinweise

Inhaltlich Verantwortliche sollten sich im Vorfeld und während einer Veranstaltung nicht mit technisch-organisatorischen Dingen befassen müssen. Daher ist das Hinzuziehen eines technisch-organisatorischen Teams sinnvoll.

Bei Veranstaltungen bis 100 ordentliche Teilnehmende scheinen zwei Helfende ausreichend, bei mehr Teilnehmenden sollte diese Zahl ggf. erhöht werden da die Helfenden nicht nur als digitale Türsteher, sondern auch als technisch-organisatorische Ansprechpartner*innen für die Teilnehmenden fungieren können. Der Kreis der Helfenden sollte sich während der Veranstaltung über einen weiteren Audio-Kanal verständigen, die Nutzung des Video-Raumes für diese Verständigung ist natürlich nicht geeignet. Als Kommunikationsinfrastruktur haben sich z.B. Discord oder Gruppenanrufe in Instand-Messenger-Diensten als hilfreich erwiesen. Die Helfenden achten dann darauf, dass ihr Mikrofon im Zoom-Raum abgeschaltet ist, wenn sie sich im Helfenden-Team austauschen und umgekehrt. Somit wird vermieden, dass die Teilnehmenden von der Veranstaltung Gespräche zwischen den Helfenden mitbekommen.

Beim Entfernen von Teilnehmenden gibt es die Möglichkeit, diese Entfernung an Zoom zu melden. Dann wird automatisch ein Screenshot erstellt, der später eingesehen werden kann. Diese Informationen sind für Ermittlungsbehörden sinnvoll.

Die Webseiten der verschiedenen Videokonferenzsystem-Anbieter bieten mittlerweile auch diverse Hinweise zur Absicherung von Videokonferenzen – eine Lektüre wird empfohlen.

Rechtliches

Seitens der nach erfolgten Störungen in Berlin hinzugezogenen Behörden (LKA / Staatsschutz) wird dringend empfohlen, jede Störung zur Anzeige zu bringen. Auch, wenn keine verfassungsfeindlichen Symbole oder anderweitig justiziable Inhalte gezeigt werden, kann immer ein , Strafverfahren wegen § 167 StGB (Störung der Religionsausübung) ‘ eröffnet werden. So die Möglichkeit besteht, sollten für digitale Veranstaltungen immer deutsche Server verwendet werden, weil die Ermittlungsbehörden dann leichter Zugriff auf die Daten der Störer erhalten können.