POLIZEI
Nordrhein-Westfalen
Kreis Mettmann

bürgerorientiert • professionell • rechtsstaatlich

# Sicherheitshinweise für Videokonferenzen

Das Nutzen von Videokonferenzen ermöglicht es, auch während der verschärften Pandemie-Bedingungen mit mehreren Personen gefahrlos kommunizieren und in Kontakt treten zu können - im privaten oder auch beruflichen Bereich. Doch bringt dies auch gleichzeitig neue Herausforderungen und Gefahren mit sich.

**Phänomen Beschreibung**
Inzwischen kommt es vor, dass digitale Videokonferenzräume auch durch unberechtigte Personen betreten werden.

Dieses Vorgehen ist inzwischen auch unter dem Begriff „*Video-Bombing*“ bekannt. Eine nicht berechtigte Person „betritt“ den digitalen Raum eines Online-Meetings. Dieses Verhalten würde man auf analoger Ebene strafrechtlich als Hausfriedensbruch einordnen. Man könnte daher auch vom „digitalen Hausfriedensbruch“ sprechen.

Je nach Meeting kann dies jedoch unangenehme Folgen haben. Zum Beispiel, dass die Fremde Person Inhalte mitbekommt, die ausschließlich privat oder für berufliche Belange bestimmt sind. Im schulischen Bereich kann die nicht berechtigte Person Kindern oder Jugendlichen durch ihr eigenes Verhalten oder dem Zeigen von verbotenen Inhalten Angst machen und sie verstören.

**Rechtliche Einordnung**
Folgende Straftaten kommen hierfür in Betracht:

**§ 202a StGB- Ausspähen von Daten** für den „digitalen Hausfriedensbruch“ bei Überwinden einer Zugangssicherung.

**§ 42 Abs. 2 Nr. 1 BDSG** - für den „digitalen Hausfriedensbruch“ ohne Überwinden einer Zugangssicherung.

**§202 c StGB- Vorbereiten des Ausspähens und Abfangens von Daten** - Weitergabe der Zugangsdaten an nicht berechtigte Personen.

**§ 201 StGB Verletzung der Vertraulichkeit des Wortes** - Unbefugtes Aufnzeichnen von Inhalten.

**§ 22; 33 KUG**
Wer Bildnisse ohne Zustimmung der Abgebildeten verbreitet.

## Wie können Sie sich schützen?

Machen Sie sich vor Beginn der Nutzung mit der Software und vor allem den Einstellungen vertraut. Insbesondere sollten Sie hier folgende Dinge berücksichtigen:

- Sichern Sie den virtuellen Raum durch ein starkes Passwort (mind. 10 Zeichen: Buchstaben/Zahlen und Sonderzeichen) ab. So erschweren Sie den Zutritt für Unbefugte.
- Verschicken Sie den Zugangs-Link und die Zugangs-Kennung getrennt voneinander
- Kontrollieren Sie den Zugang zum virtuellen Raum durch die Nutzung eines Wartebereichs und lassen Sie Teilnehmer einzeln eintreten.
- Der Wartebereich sollte nur mit eingeschalteter Kamera betreten werden, um Personen einwandfrei vor Zutrittsgewährung zu identifizieren.
- Einstellungen: Achten Sie auf die Rollenverteilung! Es gibt neben den Teilnehmenden Gastgeber und Moderatoren. Letztere haben mehr Rechte als Teilnehmer. Wo können Sie diese Rechte in den Einstellungen vergeben oder einschränken?
- Gibt es eine Aufzeichnungsfunktion und wo können Sie diese deaktivieren?
- Einstellungen: Wo und wie können Sie unerwünschte Gäste schnell entfernen und sperren?
- Nutzen Sie einen Raumnamen, der keine Rückschlüsse auf z. B. den Namen der Institution, oder bei einer Schule das Alter von Kindern zulässt.
- Datensparsamkeit: Melden Sie sich nur mit den nötigsten Daten an.
- Datensparsamkeit: Seien Sie achtsam beim Teilen des eigenen Bildschirms. Was ist im Hintergrund sichtbar oder geöffnet? Nutzen Sie die Funktion, nur einzelne Bildschirmfenster zu teilen.
- Achten Sie darauf, die Software durch Sicherheitsupdates immer aktuell zu halten.
- Als Gastgeber/Moderator sollten Sie darauf achten zum Ende des gemeinsamen Chats den Raum nicht nur zu verlassen, sondern das jeweilige den digitalen Raum auch durch Betätigen des „Beenden-Buttons“ tatsächlich zu schließen.

**Weitere Hinweise zum Aufbau eines starken Passwortes unter:**
https://www.mach-dein-passwort-stark.de/

**Tipps und Hinweise rund um das Thema Sicherheit bei Videokonferenzen:**

https://www.polizei-beratung.de/startseite-und-aktionen/aktuelles/detailansicht/5-tipps-fuer-sichere-videomeetings/

https://www.klicksafe.de/paedagogen-bereich/fuer-die-sekundarstufen/unterricht-per-videochat/