Überarbeitung der Einstellungen zur IT-Sicherheit von Zoom

Die ZIMT IT hat eine Überprüfung der Datensicherheit durchgeführt. In diesem Zuge wurden die für die Risikominimierung geeigneten technischen und organisatorischen Maßnahmen (TOM) erarbeitet und unter den globalen Einstellungen von Zoom festgelegt. Dies bedeutet, dass Einstellungen in Zoom verändert werden mussten, damit die IT-Sicherheit bei Videokonferenzen gewährleistet ist.

Die größten Veränderungen unter Zoom möchten wir Ihnen in diesem Dokument aufzeigen, damit Sie sich als Nutzer*innen von Zoom über die Änderungen informieren können.

WICHTIG: Jedes Benutzer*innen Konto wird von den Änderungen betroffen sein. Auch Konten, welche bereits seit Monaten unter Zoom und der HAWK Lizenz bestehen.

BESTEHENDE MEETINGS werden nicht geändert!
Alle Meetings, die nach der Aktualisierung der Richtlinien erstellt werden, erhalten die neuen Anpassungen automatisch.

Wir möchten Sie bitten, alte wiederkehrende Meetings erneut zu „planen“, damit diese mit den neuen Sicherheitseinstellungen ausgestattet sind. Dadurch werden der Datenschutz und die IT-Sicherheit erhöht und Ihre Meetings werden dadurch sicherer

Laden Sie den Zoom Client bitte aus dem Software Kiosk der HAWK herunter. – Im Home-Office ist dazu der VPN Client notwendig. So ist sichergestellt, dass die neuste Version installiert ist und alle Funktionen genutzt werden können.

Die Einstellungen, welche Sie auf der Website bearbeiten können, wurden von der ZIMT-IT voreingestellt, um IT-Sicherheit und Datenschutz zu gewährleisten! Diese Einstellungen sind in Abstimmung mit dem Datenschutzmanagement getroffen worden. Bitte ändern Sie hier Objekte nur, wenn Sie eine erweiterte Funktionsweise wünschen. Einige Einstellungen wurden aufgrund der Datenschutz- und IT-Sicherheitsrichtlinien gesperrt und können nicht angepasst werden. Bitte kommen Sie auf uns zu, wenn das zu Problemen führt. Wenn Sie bereits Einstellungen in ihrem Konto vorgenommen hatten, werden diese mit den aktuellen Daten überschrieben.
Weitere Handreichungen zu ZOOM finden Sie im Stud.IP der HAWK unter der Rubrik: „Lehre in Zeiten von Corona“
Bitte beachten Sie auch das PDF Dokument **„Einstellungen des Zoom-Client V2.0“**. Dort finden Sie die von der IT empfohlenen Einstellungen für den Client.

Die wichtigsten globalen Änderungen in einer tabellarischen Übersicht

Änderungen	Auswirkung	Empfehlung der IT
Keinen Zugriff mehr auf die Zoom Cloud	- Meeting Aufnahmen in die Cloud zu speichern ist nicht mehr möglich - Freigaben der hochgeladenen Aufnahmen auf der Zoom Cloud sind nicht mehr zugänglich - Download der Zoom Cloud Dateien ist nicht mehr möglich - Cloud Features nicht mehr verwendbar	- Speichern Sie Aufnahmen bitte lokal auf dem PC. (Einstellungen dazu finden Sie im Zoom Client) - Verwenden Sie keine Netzlaufwerke wie U:\ R:\ oder O:\ - Verwenden Sie die HAWK Cloud zum Teilen der Aufnahme - Holen Sie vor der Aufnahme immer das Einverständnis der Teilnehmer ein - Teilnehmer haben das Recht, die Einwilligung jederzeit zu widerrufen.
Kenncode für Meetings nötig	- Jedes Meeting muss mit einem Kenncode versehen werden - Der Kenncode wird nicht länger in dem Einladungslink eingebettet (ist wird jedoch weiterhin in der Einladungsmail von Zoom angezeigt) - Der Kenncode muss manuell vor dem Betreten eines Meetings von den Teilnehmenden eingegeben werden - Der Kenncode wird von Zoom bei dem „Planen	- Sollten Sie selbst einen Kenncode erstellen wollen, so nutzen Sie auf keinen Fall Ihr persönliches HAWK Kennwort oder sonstige Kennwörter, die Sie bereits für andere Anmeldungen verwenden.

	eines Meetings“ automatisch generiert. (Sie können dies löschen und ein eigenes Eingeben, falls dies gewünscht ist)	

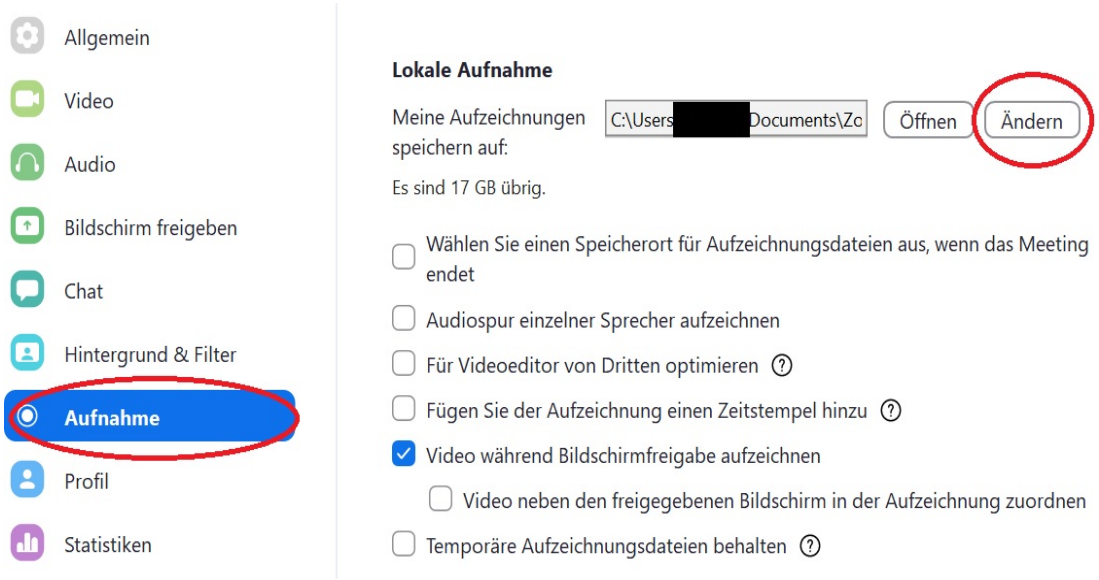
Link für Zoom in der Meeting Einladung ermöglicht die Teilnahme über den Webbrowser (ACHTUNG: Bei Verwendung des Webbrowsers sind nicht alle Funktionen nutzbar. Die IT empfiehlt die Nutzung des Clients)	- Link ermöglicht den Studierenden über das Zoom Webinterface an einem Meeting teilzunehmen - Authentifikation erfolgt über Eingabe des gesetzten Kenncodes - Anzeigename vor einem Meeting änderbar - **Eingeschränkter Funktionsumfang**	- Studierende sollten sich nicht unter Zoom registrieren - Anzeigenamen sollten nicht den realen Vollnamen enthalten. Hier wären Abkürzungen des Namens oder Sonstiges sinnvoll - Es muss dennoch eine klare Identifizierung der Teilnehmenden für den Host möglich sein. - **Die Nutzung des Clients ohne Registrierung wird empfohlen**
Nutzung des Zoom Clients ist ohne Anmeldung möglich	- Verwendung des Clients ohne Anmeldung möglich - Voller Funktionsumfang gewährleistet.	- Studierende sollten sich nicht unter Zoom registrieren - Anzeigenamen sollten nicht den realen Vollnamen enthalten. Hier wären Abkürzungen des Namens oder Sonstiges sinnvoll - Es muss dennoch eine klare Identifizierung der Teilnehmenden für den Hosts möglich sein.
End-to-End (E2EE) Verschlüsselung	- Sichere und durchgehend verschlüsselte Verbindung zwischen den	- Empfohlen bei vertraulichen Gesprächen oder Sitzungen

	Verbindungsteilnehmern via Zoom Clients. - Schlüssel nicht von Zoom oder Dritten auslesbar - ACHTUNG: Nicht alle Funktionen von Zoom stehen bei aktivierter E2EE Verschlüsselung zur Verfügung. Darunter fallen folgende Optionen: • Beitritt vor Moderator aktivieren • Einwahl per Telefon, SIP, H.323 oder Lync/Skype • Nutzung des Web-Clients oder Clients anderer Hersteller • Cloud-Aufzeichnung • Breakout-Sessions • Umfragen • Reaktionen und "Hand heben" • Live-Untertitel - Um E2EE zu aktivieren muss ein Zoom Client verwendet werden (Version 5.4.0 oder höher) - Alle Teilnehmer benötigen einen Zoom Client - Teilnahme via Webbrowser ist nicht möglich	- Für die Lehre bietet sich, aufgrund der Verluste von Funktionalitäten, die „erweiterte Verschlüsselung“ an.
Erweiterte Verschlüsselung	- Zoom Standard Verschlüsselung - Standardmäßig aktiviert - Bei Verwendung der erweiterten Verschlüsselung stehen	- Empfohlen für die Lehre, da alle Funktionen zur Verfügung stehen - Empfohlen bei großen Meetings, da die Last des Netzwerks deutlich

	alle bekannten und an der HAWK HHG freigeschalteten Zoom-Funktionen zur Verfügung. - Zugriff via Webbrowser möglich	geringer ist, als bei der E2EE Verschlüsselung.

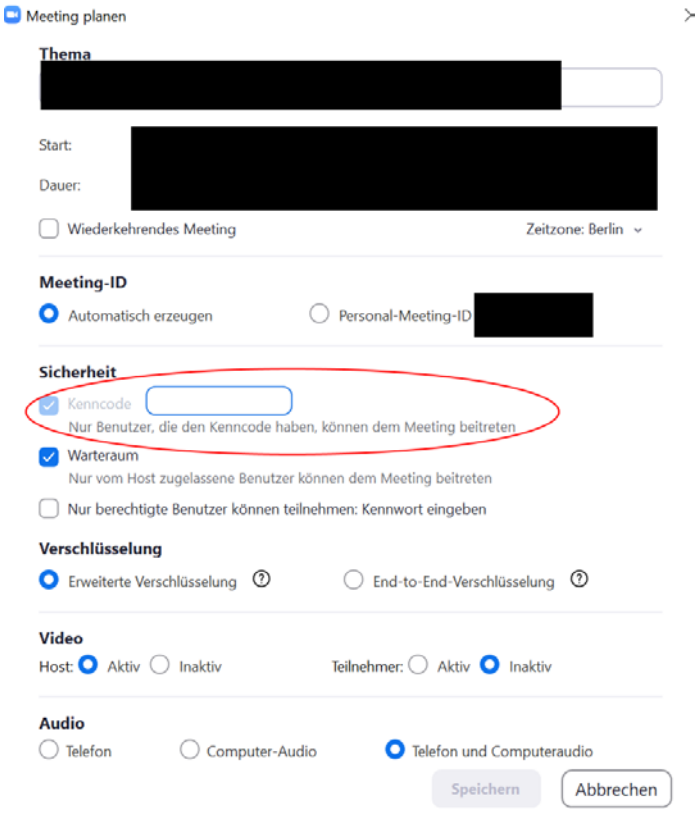
Beispiele in Bildern

1.) Lokale Aufnahme im Client einstellen
   - „Aufnahme“ ist unter den Einstellungen des Zoom Clients zu finden
   - Im Beispiel verweist der lokale Speicherort der Aufnahmen auf „Dokumente“ (die IT empfiehlt einen neuen Ordner unter den „Dokumenten“-Order zu erstellen – z.B. ein neuer Ordner mit der Kennung „Zoom“)



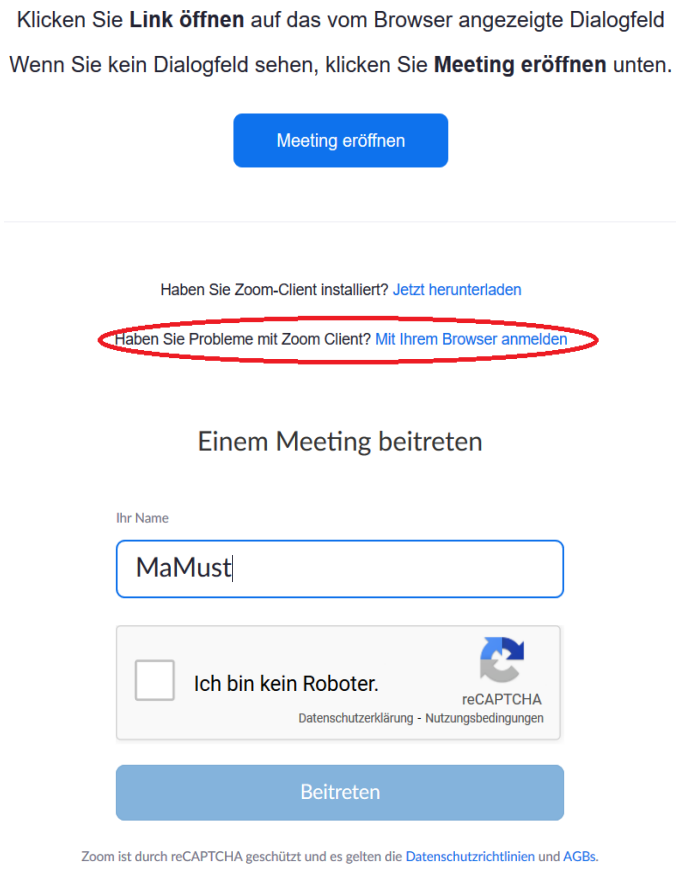
2.) Kenncode für ein Meeting einstellen

- Die IT empfiehlt den Kenncode selbst festzulegen



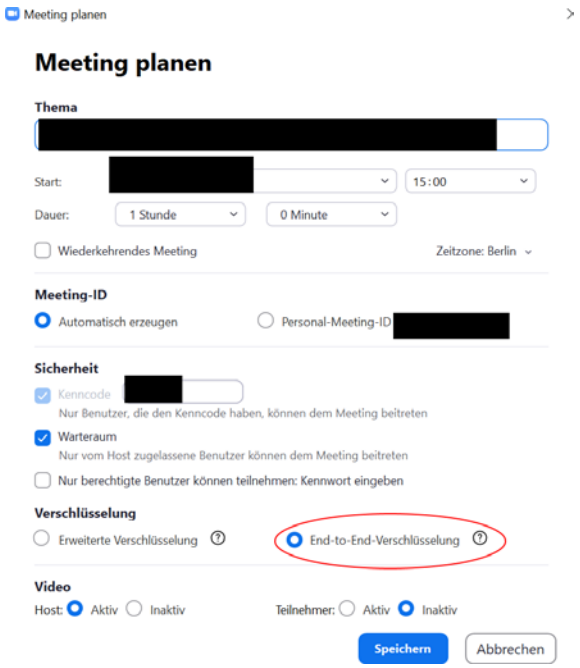
3.) Zugriff über den Zoom Web Client

- Nur eingeschränkte Funktionen möglich
- Nicht den realen Vollnamen verwenden (Die IT empfiehlt Kurznamen – im Beispiel: Max Mustermann = MaMust)
- Nach der Eingabe muss das Kennwort zum Meeting eingegeben werden
- Die IT empfiehlt das Nutzen des Zoom Clients, ohne Anmeldung



4.) Verschlüsselung

- End-to-End Verschlüsselung (E2EE)
  - **Bitte beachten Sie die Einschränkung von Funktionen unter Zoom – siehe Tabelle**
  - E2EE aktiveren



Sie können mit Ihren Meeting-Teilnehmer*innen eine Validierung der durchgehenden Verschlüsselung durchführen:

- Klicken Sie im Meeting oben links auf den kleinen grünen Schild mit dem Schloss-Icon und klicken Sie bei Verschlüsselung auf "Verifizieren".
- Bitten Sie Ihre Teilnehmer*innen, Schritt 1 ebenfalls auszuführen.
- Lesen Sie nun die Zahlengruppen vor und bitten Sie Ihre Teilnehmer*innen, die vorgelesenen Zahlen mit den Zahlen auf ihrem Bildschirm zu vergleichen.
- Wenn bei allen Teilnehmer*innen die gleichen Zahlen angezeigt werden, ist die durchgehende Verschlüsselung aktiv.