Teams meeting security FAQ

Dan Stevenson, last updated 4/6/2020

For more information, please consult the links below and see <https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide>

### Data security for audio/video traffic

* Network communications in Teams are encrypted by default using TLS, SRTP, and other industry standards, including 256-bit AES. Media traffic uses SRTP both for client-to-client calls and multi-party meetings
* Key exchange (using PKI on Windows Server) is also done using TLS

## Managing meeting securely

* Control who can join directly: restrict to company employees, employees and managed guests, or everyone
  + Set at an organization level using organization-wide meetings settings: <https://docs.microsoft.com/microsoftteams/meeting-settings-in-teams>
  + Or set on a per-user level using meetings policies (see below)
  + All other access is managed via a meeting lobby
* Control what people can do in the meeting
  + Presenters can do more than attendees, e.g. take control, share screen
  + Configure who can be a presenter via meeting options (click from the meeting in Teams or Outlook)
* Set policies for meetings (see <https://docs.microsoft.com/microsoftteams/meeting-policies-in-teams>)
  + Create different policies for different sets of users
  + Control who can start or schedule a meeting, and how
  + Block/allow recording and transcriptions
  + Block/allow video sharing in a meeting (can apply selectively so some users in the meeting can share, but others cannot)
  + Block/allow screen sharing, PowerPoint sharing, whiteboard, and meeting notes

### Meetings data security

* Files shared in a meeting
  + If a file is uploaded to a meeting, or shared via PowerPoint sharing, then all meeting participants inside the company will have access to it (if shared in a channel meeting, then all channel members will have access to it)
  + No access is granted to files shared via screen sharing (these files may have been separately shared, outside of the meeting)
  + More information on sharing files on OneDrive and SharePoint: <https://docs.microsoft.com/onedrive/manage-sharing>
* Meeting recording and transcript
  + Meeting recordings created in Teams are stored in the cloud storage for Microsoft Stream
  + The organizer and all meeting participants inside the company have access to the recording
  + Meeting recordings are not published online for public access
  + Meeting recordings include the shared group chat messages but do not include any other private messages among meeting participants
  + The person who initiated the recording is the only one who can download the recording or share it with others, including those outside the organization
  + More information on meeting recordings: <https://docs.microsoft.com/microsoftteams/cloud-recording#where-your-meeting-recordings-are-stored>, <https://support.office.com/en-us/article/Play-and-share-a-meeting-recording-in-Teams-7d7e5dc5-9ae4-4b94-8589-27496037e8fa>

### Teams Live Events security

* Control who can create a Live Event
  + Use Live Events policies to configure which users are allowed to create Live Events: <https://docs.microsoft.com/en-us/MicrosoftTeams/teams-live-events/set-up-for-teams-live-events>
  + Also configure defaults for recording, transcription, and who can join (see below)
* Control who can join a Live Event
  + Meeting organizers can determine if the Live Event is open to all public attendees, only people in the organization, or only to specific people
  + More information: <https://support.office.com/en-us/article/get-started-with-microsoft-teams-live-events-d077fec2-a058-483e-9ab5-1494afda578a>
* Live Events recording, transcript, and attendance report
  + Participants can join a Live Event afterwards and watch it (same restrictions on "live" attendance)
  + Only the organizer can download and share the recording file; same for attendance report, Q&A report, and transcript - see <https://support.office.com/en-us/article/Manage-a-live-event-recording-and-reports-in-Teams-6d1f5da9-74b7-4771-977d-b89eba194578>