ZOOM.US Security

ZOOM.US was originally heavily criticized because of security vulnerabilities. However, from April 2020 onwards, ZOOM announced strong improvement measures, which have already been implemented to a large extent. A report on transparency at ZOOM is still pending. This is to be presented by the end of the year.

The ZOOM.US security plan
Since April, ZOOM has established a security plan with milestones, which includes various points to be implemented within 90 days. All promises from the security plan have been kept.
In this context, ZOOM has also stopped all software developments that were associated with security concerns.

On the security concept:

- Encryption: ZOOM will use AES 256 GCM Transport encryption in the future. This mode is considered one of the most secure encryptions
- Each videoconference is password protected
- ZOOM waiting rooms help to keep unwanted people out of meetings
- Screen sharing can be restricted
- Faster response time to detect security breaches and resolve them more quickly
- Persons who violate the respective rules can be reported to ZOOM
- Security functions are clearly highlighted in the ZOOM settings

*** On August 7th, 2020, a ZOOM.US webinar was held with Head of ZOOM Germany Peer Stemmler and Federal Data Protection Commissioner Prof. Ulrich Kelber. During this webinar both Mr. Stemmler and Prof. Kelber answered questions from the audience.
Among other things, they talked about the Privacy Shield, which does not comply with the guidelines of the DSGVO. Furthermore, it was clarified once again that all data stored on US servers can also be used and viewed by companies and the government. According to ZOOM, the following therefore applies: If you do not want your data to be passed on and processed in the USA, you must create an account with ZOOM.US for a fee and select the server for meetings and webinars.

Problems ZOOM had before and how they were solved:

1. Allegations that ZOOM data was forwarded to Facebook

Apple devices used the Facebook Software Development Kit when downloading ZOOM. ZOOM has now removed this from the software and is no longer included in new updates.

2. ZOOM Bombing

Because of insufficient security around meeting, it was possible for people tob arge into meetings. However, it is now possible to make this more difficult with different settings
These include:

- Activation oft he waiting room by default
- Setting of passwords by default
- Restrictetions on who is allowed to share their screen
- (registering for meetings)

This is said to have made it over 1000 times more difficult to attend a meeting illegally.

3. Leakted ZOOM-Accounts

You should choose an individual and complex password for your own account to protect yourself from hackers.

4. Selecting a Data Center

Due to the increasing number of users of ZOOM.US, data centers were provided in various countries. Paying users can decide which server should be used for a conference.

https://dataloft.ch/security/zoom-stellt-neuen-plan-fuer-sicherheit-auf/
https://www.pc-magazin.de/ratgeber/zooom-sicher-nutzen-videokonferenz-sicherheit-tipps-3201560.html
https://blog.zoom.us/zoom-hits-milestone-on-90-day-security-plan-releases-zoom-5-0/
https://www.heise.de/security/meldung/Sicherheitsupdate-Angreifer-koennten-Schadcode-in-Zoom-Meetings-schieben-4774257.html
https://www.funkschau.de/office-kommunikation/sicherheitsupdates-mit-zoom-5-0.175874.html
https://www.heise.de/security/meldung/Videokonferenz-Software-Ist-Zoom-ein-Sicherheitsalptraum-4695000.html
https://blog.to.com/zoom-in-der-kritik/