National Cyber Security Centre

Securing video conferencing services

Micro exercise

Exercise introduction

This micro exercise is focussed on video conferencing services. It is a short and sharp session that explores this topic using a combination of interactive activities to cover the risks associated with the use of video conferencing services and what you can do to help secure your use of these services. You will have the opportunity to evaluate yourselves as a group against various competencies and at the end of the exercise you will be provided with a report summarising your evaluation.

Participants and timing

Allow around 15 to 30 minutes, you may choose to tailor this to the time you and your participants have available.

Required attendees

You can have as many or as few people involved as you like, and no one taking part in this exercise needs to be a cyber security expert. We recommend 3-5 people including a nominated facilitator to run the session and keep the conversation on track.

What is expected of the participants?

You're here to think, talk and learn about this topic. You don't need to be a cyber security expert; it is not a test. Instead, we aim to enable collaborative discussions that further your knowledge and help you identify areas of improvement.

Your nominated facilitator is here to run the session and keep the conversation on track, in whatever way the group is comfortable with.

All material is UK Crown Copyright ©

Context

With more staff now working remotely, there is a significant increase in the use of video conferencing and collaboration services to hold team meetings, brief clients etc. There are several providers to choose from and staff may be familiar with one but not with others.

The increase in use of these services has highlighted them to attackers, who may wish to cause annoyance or offence, gather information, or steal data. For example, lack of controls on a video conference can lead to unauthorised individuals joining a meeting.

This micro exercise highlights some of the risks associated with the use of video conferencing services and explores what you can do to help secure your use of these services.

All material is UK Crown Copyright ©

Questions

Question 1 of 3

If you wanted to sign up for a new video conferencing service, what security considerations should you think about?

All material is UK Crown Copyright ©

Answer

Consider how the provider implements basic security controls, such as the ability to set strong passwords for meetings

Look at what features they have available for hosts to protect their meetings from unwanted guests, such as waiting rooms

Review whether they offer end-to-end encryption, protecting your video calls between yourself and your participants

Research if they offer the ability to blur your background or apply custom backgrounds.

The free version of a video conferencing service will probably provide sufficient functionality and security for personal use. Some providers also offer paid options that can include more features and enhanced security options which may be more appropriate for the types of meeting you are planning to hold

All material is UK Crown Copyright ©

Question 2 of 3

Video conferencing obviously allows you to see and talk to participants, but what other functionalities often feature within video conferencing services?

All material is UK Crown Copyright ©

Answer

- File sharing
- Chat and raise hands
- Screen sharing
- Switch video and audio on or off
- Ability to record chat and video and to generate a call transcript
- Ability to control another participant's device

All material is UK Crown Copyright ©

Question 3 of 3

What steps can you take to facilitate confidentiality, before and during a video conference meeting?

All material is UK Crown Copyright ©

Answer

- Do not share meeting links with others on social media. Private messaging apps are a better alternative to ensure that meeting invites are limited to intended attendees.
- Ensure you have a waiting room/lobby set up and only admit people authorised to be there.
- When you are sharing your screen be aware of what other windows and documents might be displayed to others.
- Reduce the possibility of a data leak by disabling file sharing options before your video conference starts. If required, the meeting organiser can later enable the functionality for attendees.
- Consider changing your background to provide some personal privacy.

All material is UK Crown Copyright ©

Scenario

Consider the scenario outlined and run through the remaining points when you are ready.

The Scenario

You are facilitating a video conference between your company and an important client. You have sent out links and meeting details to the attendees and configured a waiting room for participants to join before they enter the meeting. Someone enters the waiting room with a display name that you do not recognise.

What to consider

What would you do in this scenario?

- What might be the repercussions if you admit them to the conference and they are an unauthorised attendee?
- Should you just remove them from the waiting room?

All material is UK Crown Copyright ©

Your Response

Answering **Yes** or **No,** would you ask the others in the conference or your colleagues if they can verify who the participant is before you admit them?

Discuss this as a group and consider what your answer would be.

The potential impacts of answering **Yes** or **No** will be revealed on the next pages.

All material is UK Crown Copyright ©

Responding “Yes”

- You should always ascertain the identity of any participants you do not recognise.
- Consider attempting to contact any missing attendees using other communication channels, to check if they are attempting to join with the unrecognised display name.

All material is UK Crown Copyright ©

Responding “No”

- The increase in video conferencing has enabled a new type of malicious behaviour that involves uninvited individuals joining calls, sharing distressing content to participants, and causing disruption. This can have a serious impact on organisations, educational institutions, and social groups.
- You should always verify participants before you admit them to the conference.
- Removing them from the waiting room could cause issues if they are an authorised attendee and they try to re-join the conference.

All material is UK Crown Copyright ©

Advice

- Consider setting company-wide defaults and controls on the service that adhere to internal policies.
- Ensure that controls are in place, such as a meeting waiting room and/or locking the room. This helps to ensure that meetings avoid unwanted interruptions or unauthorised individuals joining the video conference.
- Meeting owners should verify and approve participants in the lobby/waiting room and remove those who are not identified or authorised.
- Account owners and administrators should ensure monitoring and logging is in place.
- Like other types of software, video conferencing applications should be kept up to date.
- Consider where you set up for video conferencing, for example setting up near a window or near others on public transport can impact the confidentiality of a meeting.
- Be aware of any request to take remote control of another participant's device. Ensure that the reason for the request is understood and reasonable before granting the request.
- Think about what the camera can see, consider blurring your background or using a virtual background.
- Ensure that you only download the video conferencing software from trusted sources, for example, from the official website or from your phone/tablet's official app store.
- If your organisation is choosing a new video conferencing service, you should review the NCSC's SaaS security principles.

All material is UK Crown Copyright ©

Evaluation

Discuss the following statements and rate them on a scale of:

1. Not at all confident
2. Slightly confident
3. Somewhat confident
4. Fairly confident
5. Completely confident

- We have organisational policies and guidance in place to support users with video conferencing.
- We can share meeting invites securely.
- We can create a waiting room or lobby for participants.
- We know how to verify and remove a participant from a video conference.

All material is UK Crown Copyright ©

Conclusion

Video conferencing has become a fundamental tool for home and remote working recently with significant growth in the use of the software. However, this has created additional opportunities for attackers to carry out a range of attacks, ranging from annoyance to exploitation of systems.

It is important to choose the most suitable provider for your organisation and ensure that software is configured appropriately and updated regularly to protect company data.

More top tips and guidance on this topic can be found on the NCSC website.

All material is UK Crown Copyright ©

Next steps

Make recommendations that will develop confidence in the areas that have been identified as having scope for improvement. Areas for improvement could be where you have given a lower confidence rating in any of the exercise observations. Discuss with and allocate the recommendations to the people in your organisation who can facilitate change and action improvement. Discuss the risks associated with not addressing the recommendations.

Ensure any recommendations are implemented and when ready, run the exercise again to see how those changes have impacted upon your organisation.

Also refer to the Related Guidance, below, which may help you in those areas you have identified as needing improvement.

To run further exercises please go back to Exercise in a box.

All material is UK Crown Copyright ©

Related guidance from the NCSC

Small Business Guide - How to improve cyber security within your organisation - quickly, easily and at low cost.
Small Business Guide: Response and Recovery - Guidance that helps small to medium sized organisations prepare their response to and plan their recovery from a cyber incident.
Mitigating Malware - This guidance describes how organisations of all sizes - and home users - can reduce the likelihood of being infected by malware.
Recovering a hacked account - Guidance explaining what you can do to minimise the damage, and how you can regain access to your accounts.
Home working: preparing your organisation and staff - How to make sure your organisation is prepared for home working.
Video conferencing services - Guidance to help you to choose, configure and deploy video conferencing services within your organisation.
Software as a Service (SaaS) - How to choose, configure and use cloud services securely, specifically the cloud security principles.

All material is UK Crown Copyright ©