Angriffsziel Videokonferenz

Warum Informationssicherheit bei „Online Meetings“ so wichtig ist!

Online-Meetings, die z. B. über Microsoft Teams, Zoom oder Cisco Webex abgehalten werden, sind aus dem Arbeitsalltag nicht mehr wegzudenken. Allerdings gibt es beim Einsatz derartiger Kommunikationstechnologien auch große Herausforderungen, weil u. a. sicherheitsrelevante Attacken auf ebendiese Technologien überproportional ansteigen.

Darauf macht Markus Vollmuth, Informationssicherheitsberater bei der atarax Unternehmensgruppe, aufmerksam. Einerseits nutzen Cyberkriminelle die Situation, dass viele Mitarbeiter der Unternehmen von Zuhause oder remote arbeiten, um Phishing-Angriffe und Cyberattacken zu platzieren. Andererseits besteht das Risiko, dass die Organisatoren und Teilnehmer der Online-Meetings versehentlich sensible Informationen veröffentlichen, wenn sie sich nicht an vorgegebene Sicherheitsregeln halten.

Für eine hohe Sicherheit bei Videokonferenzen sollten Sie nachfolgende Tipps beachten.

Sorgfältige Vorbereitung

Neben den Grundsätzen aller Meetings, das heißt entsprechende Vorbereitung mit Zielsetzung, Agenda und Ergebnisprotokoll, gibt es weitere Punkte zu beachten. Die Gefahr einer unbeabsichtigten Offenlegung schützenswerter Informationen oder personenbezogener Daten ist bei virtuellen Meetings naturgemäß größer.

- Bei internen Meetings sollten **nur registrierte Teilnehmer** akzeptiert werden.
- **Meeting-Links** und **Einwahlcodes** sollten **gut geschützt** und nicht auf öffentlichen Plattformen geteilt werden.
- Bei Meetings mit externen Teilnehmern sollte ein **„Warteraum“** genutzt werden, in dem die externen Teilnehmer zunächst warten müssen, bis der Gastgeber/Organisator den Beitritt akzeptiert und diese gezielt verifizieren kann.
- **Akustische Signale**: Das System sollte so konfiguriert sein, dass es bei jedem Eintritt eines Teilnehmers ein akustisches und/ oder sichtbares Signal gibt.

Durchführung des Meetings

Ist die Vorbereitung abgeschlossen, sollten Sie einige Regeln im Hinblick auf die Durchführung aufstellen.

- **Start:** Meetings sollten stets mit ausgeschalteter Audio- und Videoübertragung gestartet werden, um unbewusste und versehentliche Übermittlungen zu vermeiden.
- **Beitritte:** Teilnehmer sollten überprüft werden und der Eintritt sollte nur aktiv zugelassen werden.
- **Entfernen:** Unbekannte bzw. nicht eindeutig identifizierte oder unerwünschte/ unbenötigte Teilnehmer sollten entfernt werden.
- **Screen-Sharing:** Teilnehmer sollten nicht ihren kompletten Bildschirm, sondern nur bestimmte Applikationen teilen, um versehentliche Leaks zu vermeiden. Sollte es dennoch nötig sein, den Bildschirm zu teilen, ist auf einen aufgeräumten Desktop zu achten.
- **Verschlüsselung:** Setzen Sie Verschlüsselungstechnologien bei der Übertragung ein.
- **Aufnahme ausschließen:** Erlauben Sie standardmäßig keine Aufnahmen des Meetings. Falls Aufnahmen der Meetings notwendig sind, unterrichten Sie im Vorfeld alle Teilnehmer dazu und holen Sie die entsprechenden Einwilligungen ein. ■

Autoren: Rico Seyd, IHK zu Coburg, Markus Vollmuth, atarax Unternehmensgruppe

Kontakt
Rico Seyd, Tel.: 09561 7426-46
E-Mail: rico.seyd@coburg.ihk.de