▶ Digitalisierung

BSI empfiehlt Verschlüsselung, 2FA oder P2P für (anwaltliche) Videokonferenzen

von RA Dr. Stefan Rinke, Berlin

| Im aktuellen Lagebericht zur IT-Sicherheit in Deutschland 2021 weist das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf Schwachstellen in der IT-Sicherheit hin (iww.de/s5767). Doch Verschlüsselung, 2FA und P2P sind ein wirksamer Schutz für Videokonferenzen. |

INFORMATION
BSI-Lagebericht
iww.de/s5767

Bei der Digitalisierung besteht Nachholbedarf

BSI weist auf Bezug von Videokonferenzen und IT-Sicherheit hin

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) leitet seinen Lagebericht zur IT-Sicherheit in Deutschland 2021 mit der Relevanz von Videokonferenzen und IT-Sicherheit ein: „Die Coronapandemie hat den Alltag vieler Menschen in den vergangenen anderthalb Jahren erheblich verändert. Und sie hat gezeigt, dass wir bei der Digitalisierung in Deutschland Nachholbedarf haben. Als Gesellschaft haben wir Prioritäten neu gesetzt und viele unserer Gewohnheiten angepasst: Wir haben uns an die AHA-Regel gewöhnt, im Homeoffice und beim Homeschooling eingerichtet, Videokonferenzen und virtuelle Familientreffen abgehalten. Viele dieser Neuerungen werden uns auch nach der Pandemie begleiten. Daher ist es angebracht, sich auch mit den zugehörigen Herausforderungen auseinanderzusetzen, insbesondere im Bereich der Informationssicherheit."

Eklatantes Beispiel: „Zoom-Bombing" auf EU-Verteidigungsminister

Die Herausforderung seien immer ausgefeiltere Cyber-Angriffe, auch auf Videokonferenzen. Zwar sei Deutschland bislang noch in einem geringeren Ausmaß betroffen als andere Länder. IT-Systeme sind aber auch hier verwundbar. Das zeigt sich nicht zuletzt in Bezug auf die Videokommunikation, wenn sich z.B. „Angreifer mittels zuvor erlangter Zugangsdaten unerkannt in Videokonferenzen einwählten und interne Informationen abgreifen konnten." Eklatantes Beispiel ist das „Zoom-Bombing" einer Konferenz der europäischen Verteidigungsminister.

Das sind die Schutzmöglichkeiten bei Videotelefonie

1. Möglichkeit: 2FA

Eine Möglichkeit, Kommunikationsinhalte und Daten in der Videotelefonie zu schützen, ist die Zwei-Faktor-Authentifizierung (2FA). Als Methode zum Nachweis der Identität eines Nutzers gilt sie durch die Verwendung zweier unterschiedlicher und unabhängiger Faktoren als sehr sicher, z. B. durch Passwort und separat generierte TAN. Auch wenn Zugangsdaten aus Versehen öffentlich werden, ist der Schaden aufgrund des fehlenden zweiten Faktors gering.

2. Möglichkeit: P2P

Zusätzliche Sicherheit lässt sich auf technischer Ebene erreichen. Mögliche Angriffspunkte für Cyber-Kriminelle sind häufig Server, über die Kommunikationsdaten weitergeleitet werden. Eine Peer-to-Peer-Verbindung (P2P), also ein direkter Kommunikationskanal zwischen den Gesprächspartnern ohne Server, verhindert dies. Sensible Gesprächsinhalte werden dabei sicher verschlüsselt ausgetauscht, ohne Zugriffsmöglichkeit für nicht autorisierte Personen. (Quelle: RA-MICRO News, mehr lesen unter iww.de/s5774)