Sichere Nutzung von Videokonferenzen und Online-Seminaren - Sinnvolle Tipps zum Sicherheits- und Datenschutz-optimierten Einsatz

DresPleier GmbH, 84149 Velden, Deutschland

Videokonferenzen und Online-Seminare bieten viele Vorteile wie keine Reisekosten oder Wegzeiten nötig, freiere Terminwahl möglich, Lernen in gewohnter Atmosphäre zu Hause oder im Büro und andere. Sie stellen besondere Anforderungen an Sicherheit und Datenschutz, da Daten wie Audio, Video, Desktop usw. über das Internet übertragen werden können und dabei ungewollte, zu viele oder zu sensible Daten übertragen und an unberechtigte Dritte gelangen können. Dem Nutzer, seinem Bewusstsein und Handeln, kommt hierbei ein großer Stellenwert zu. Dieser Artikel beleuchtet Nutzer-fokussiert sinnvolle Tipps zum geschützten Einsatz.

Der Artikel konzentriert sich auf die Nutzeraspekte bzw. Nutzung. Voraussetzung ist also, das Client- und das Videokonferenz-System sind gesichert. Nachfolgend eine Beschreibung, worauf es als Nutzer ankommt, bei der Nutzung von Videokonferenz-Systemen, egal ob für Videokonferenzen oder Online-Seminare. Diese erfolgt allgemein und nicht auf bestimmte Systeme bezogen, damit ohne Details zu einzelnen Systemen. Die Anregungen sind kurz und griffig dargestellt als Handlungswort, -beschreibung und -erklärung, gegliedert in die Phasen vorher, während, nachher und können daher wie eine Checkliste genutzt werden.

***** vorher *****

Nutzenabwägung -
Wägen Sie den Nutzen ab, nutzen Sie ggf. Präsenzalternativen oder reduzierte Funktionen
Als Nutzer haben Sie Vorteile, senden jedoch Daten über das Internet. Es existieren Alternativen wie Präsenzunterricht oder -beratungen. Zudem sind Videokonferenzen Datenschutz-optimiert nutzbar (z.B. keine Verwendung zusätzlicher Funktionen wie Chat). Auch Telefonkonferenzen sind möglich, falls ein Sehen der Teilnehmer oder Übertragen von Präsentationen nicht nötig ist.

Mitdenken -
Agieren Sie intelligent, denken Sie mit bei dem, was Sie tun
Grundsätzlich ist ein Mitdenken sinnvoll, was man tut bzw. unterläßt. Achten Sie auf ein Sicherheits- und Datenschutz-optimiertes Handeln. Denken Sie vorher über neue Funktionen nach, nutzen Sie diese nicht einfach, weil sie vorhanden sind bzw. angeboten werden.

Informieren -
Lesen Sie vorab die Videokonferenz-spezifischen Informationen des Organisators
Tipps zur Nutzung, Informationen zum Datenschutz und andere Informationen helfen Ihnen. Überlegen Sie sich vorher, welche Funktionen Sie nutzen bzw. freigeben wollen oder nicht, damit Sie nicht durch Marketing des Providers oder Gruppendynamik mehr tun als gewollt.

Pseudonymisierung -
Nutzen Sie ggf. Pseudonymisierung für Ihre Zugangsdaten
Verbergen Sie gegebenenfalls Ihre personenbezogenen Informationen geeignet indem Sie keine "sprechenden" Mail-Adressen, Klarnamen oder Ähnliches verwenden.

Zugangsschutz -
Schützen Sie die Videokonferenz und Zugangsdaten vor unberechtigter Nutzung
Die Videokonferenz sollte nur berechtigten Teilnehmern, dazu nur mit einer Zugangsberechtigung nutzbar sein wie passwortgeschützte Kennung, Besprechungs-ID mit Zusatzcode oder Ähnliches. Nutzen Sie hierzu sichere Passwörter, IDs usw. und schützen Sie diese[1].

1 Siehe hierzu auch DresPleier GmbH: DresPleierPwS - Passwörter nicht-digital sicher speichern und verwenden; www.DresPleier.de

Client-Nutzung -
Nutzen Sie Videokonferenz-Clients, keine Browser für Videokonferenzen
Nutzen Sie das Videokonferenz-System Client-basiert, also nicht via Browser, da Browser-Links leichter gehackt, gestohlen, missbraucht werden können. Ideal ist also ein dedizierter Client mit dediziertem Login und Betreten der Videokonferenz.

Einstellungsoptimierung -
Stellen Sie Ihren Videokonferenz-Client und die Videokonferenz gesichert ein
Befassen Sie sich angemessen mit den Einstellungen, die Sie selbst am Client konfigurieren können und stellen Sie diese möglichst sicher ein, also z.B. kein automatisches Starten der Client-Software beim Rechnerstart. Die Einstellungen sind bei Aktualisierungen der Client-Software regelmäßig zu prüfen, ob sie noch in Ordnung sind oder geändert wurden oder neue Funktionen bzw. Einstellungen vorhanden sind. Organisieren Sie die jeweilige Videokonferenz, so konfigurieren Sie diese auch möglichst sicher, z.B. ohne Chat-Funktion.

Rechnerschutz -
Sicherheitsoptimieren Sie Ihren Rechner
Nutzen Sie idealerweise einen eigenen Videokonferenz-optimierten Rechner. Räumen Sie diesen auf (Desktop, gespeicherte Daten usw.) und schließen Sie alle nicht benötigten Anwendungen (insbesondere mit potentiell sensiblen Informationen). Für weitere Funktionen wie Mails nutzen Sie am besten einen zweiten Rechner neben dem Videokonferenz-Rechner, so daß ein Schutz durch physische Trennung gegeben ist.

Umgebungsschutz -
Sicherheitsoptimieren Sie Ihre Umgebung (Schreibtisch, Wand, ...)
Durch die Übertragung können schützenswerte Informationen an Unberechtigte gelangen. Bereiten Sie daher Ihre Umgebung geeignet vor. Nutzen Sie idealerweise einen dedizierten, Umgebungs-unkritischen Raum für Ihre Videokonferenz, ansonsten positionieren Sie den Rechner bzw. die Kamera so, daß nur "übertragbare" Objekte aufgenommen werden können oder stellen Sie einen Sichtschutz auf. Lassen Sie keine sensiblen Informationen (z.B. Zettel mit Passwörter) im Kamera-Sichtfeld[2], verschleiern Sie gegebenenfalls Ihren Hintergrund[3]. Berücksichtigen Sie einen erweiterten Erfassungsraum der Kamera, dabei auch Veränderungen der Kamerapositionierung in der Videokonferenz (z.B. durch Drehen des Laptops).

Anderenschutz -
Schützen Sie Andere vor unabsichtlicher Audio- oder Video-Übertragung
Andere Personen könnten unwissend in den Kamera- oder Mikrofon-Aufnahmebereich geraten. Nutzen Sie daher einen abgegrenzten Videokonferenz-Raum, hängen Sie einen Zettel als Warnung an die Tür, damit nicht unabsichtlich Kollegen, Familienmitglieder oder Andere in die Übertragung geraten. Auch laute Gespräche im Nebenraum könnten erfaßt werden.

Außenwirkung -
Achten Sie auf eine angemessene Außenwirkung (Aussehen, Kleidung, Umfeld)
Für Videokonferenzen ist eine passende Außenwirkung, auch als Eigenmarketing wichtig. Sehen Sie gepflegt aus, tragen Sie angemessene Kleidung, achten Sie auf die Wirkung Ihres Hintergrundes. Prüfen Sie vorab Ihr Videobild, was alles wie erfaßt bzw. übertragen wird und wie es wirkt.

Qualitätssicherung -
Nutzen Sie eine Checkliste, um Wichtiges qualitätsgesichert zu tun
Erstellen Sie sich eine individuelle Kontrolliste mit dem Wichtigsten zu beachten, z.B. vor Beginn der Videokonferenz alle sensiblen Objekte/Unterlagen aus dem Kamerabereich entfernen, Hinweis an der Tür anbringen "Achtung Videokonferenz!", daran denken, keine Passwörter vor laufender Kamera einzugeben usw.

2 Achtung: Die Kamera kann möglicherweise mehr aufnehmen als Ihnen angezeigt wird

3 Hierbei wir die Person gegenüber dem Hintergrund ermittelt und alles zum Hintergrund gehörige entweder verschleiert oder durch ein Bild ersetzt. Aus Gründen der Performance wird dies meist beim Videokonferenz-Provider erfolgen, d.h. die gesamte Videoaufnahme dorthin übertragen, dann umgewandelt und verteilt. Der Provider kann daher alles von der Kamera Aufgenommene, gegebenenfalls auch Sensibles, erlangen. Zudem kann diese Funktion während der laufenden Videokonferenz temporär fehlerhaft sein. Besser ist daher, den Raum, Tisch usw. vorab sicherheitszuoptimieren.

***** während *****

Nutzungsaktivierung -
Starten Sie die Videokonferenz-Software nur bei der Durchführung
Vermeiden Sie ungewollte Funktionen oder Aktivitäten des Videokonferenz-Systems wie kein automatisches Starten beim Rechnerstart oder kein automatisches Annehmen eines Videoanrufs.

Teilnehmerprüfung -
Achten Sie auf die Teilnehmer, daß nur Berechtigte teilnehmen
Beobachten Sie regelmäßig in der Videokonferenz, wer teilnimmt und ob jemand dazukommt. Erkennen Sie Unberechtigte möglichst sofort.

Funktionsüberprüfung -
Prüfen Sie die Funktionen des Videokonferenz-Systems auf korrekte Arbeitsweise
Qualitätssichern Sie die einzelnen Funktionen Nutzer-seitig, also z.B. ist eine Videoübertragung auch wirklich aus, sofern sie deaktiviert ist, stimmt die Anzeige (Mikrofon an/aus) auch mit der Funktionalität überein usw.

Übertragungssteuerung
Aktivieren Sie Video-, Audio-, Anwendungs-, Desktop-Übertragung bedarfsorientiert
Minimieren Sie die Übertragung zum Start bzw. Betreten der Videokonferenz (kein Audio, Video, Anwendung, Desktop wird übertragen). Aktivieren Sie Übertragungen gesteuert und bedarfsorientiert und nur, wenn keine sensiblen Informationen übertragen werden (also z.B. keine vertrauliche Mail gerade geöffnet ist). Nutzen Sie gegebenenfalls alternative Übertragungsmöglichkeiten wie verschlüsselte Mails. Geben Sie nicht die Steuerung Ihres Desktops an andere Teilnehmer ab, um einen potentiellen Missbrauch zu vermeiden.

Datenminimierung -
Nutzen Sie keine unnötigen Funktionen des Videokonferenz-Systems
Beachten Sie das bewährte Prinzip der Einfachheit (KISS-Prinzip). Setzen Sie das Videokonferenz-System grundsätzlich dafür ein, wofür es gedacht ist: Die Übertragung von Video und Audio sowie Präsentationen zwischen den Teilnehmern. Verzichten Sie auf überladene Funktionen wie Chat, Ablage von Dokumenten oder Ähnliches im Videokonferenz-System und lassen Sie sich auch nicht dazu verführen durch den Provider oder andere Teilnehmer. Nutzen Sie keine Zusatzübertragungsmöglichkeiten des Videokonferenz-Providers, also z.B. keine Dateiübertragung. Verwenden Sie bei Bedarf gesicherte und von Ihnen kontrollierte Alternativen, z.B. Datenablage auf dem Firmenserver oder verschlüsselte Mail. Verzichten Sie zudem auf eine Sprachsteuerung, da diese permanent Audio mitverfolgen kann.

Vertraulichkeitsschutz -
Geben Sie keine vertraulichen, schützenswerten Informationen preis
Sagen Sie keine Passwörter oder anderes Vertrauliches bei aktivierter Audio-Übertragung, es könnte so kompromittiert werden. Geben Sie keine Passwörter bei aktivierter Kamera ein, sie könnten so ausgespäht werden; deaktivieren Sie die Kamera oder (besser!) decken diese physisch zu oder führen die Eingabe verdeckt durch. Halten Sie keine vertraulichen Dokumente vor die Kamera, sie könnten so kompromittiert werden. Beachten Sie dazu auch andere Tipps wie Datenminimierung.

Aufzeichnungsschutz -
Zeichnen Sie keine Übertragungen (Video, Audio, Anwendung/Desktop) auf
Dem müssten alle Teilnehmer vorab zustimmen. Achten Sie während der Videokonferenz auf die Anzeige einer gegebenenfalls aktivierten Aufzeichnung (Symbol oder Ähnliches), um dies sofort erkennen und abbrechen zu können.

***** nachher *****

Datenlöschung -
Löschen Sie alle überflüssigen oder temporär erzeugten Daten
Räumen Sie auf. Entfernen Sie nach der Videokonferenz alle dabei erzeugten Daten geeignet.

Systemabmeldung -
Melden Sie sich aus dem Videokonferenz-System über die Abmeldefunktion sicher ab
Melden Sie sich sicher ab, um eine unberechtigte Nutzung zu verhindern.

Client-Terminierung -
Beenden Sie das Programm sicher und vollständig
Beenden Sie das Videokonferenz-System bzw. den Client vollständig und vermeiden Sie ungewollte Funktionen oder Aktivitäten des Videokonferenz-Systems.

Physischer Schutz -
Schützen Sie sich vor Missbrauch via Kamera oder Mikrofon
Sichern Sie Ihr Gerät, z.B. durch physischen Schutz wie zudecken der Kamera oder einen Dummy-Stecker beim externen Mikrofonanschluß.

Datensicherung -
Schützen Sie übertragene bedeutsame Daten durch einen zweiten Weg
Daten, die via Videokonferenz-System übertragen werden, könnten verfälscht werden, auch live/ inline durch Angreifer des Videokonferenz-Systems, was insbesondere bei Vertragsverhandlungen sehr bedeutsam sein kann. Nutzen Sie daher für Wichtiges einen zweiten Kanal außerhalb des Videokonferenz-Systems zur Bestätigung des Übertragenen.

Fazit

Videokonferenzen und Online-Seminare bieten viele Vorteile wie Sparen von Reisekosten oder Wegzeiten, freiere Termingestaltung, Lernen in gewohnter Atmosphäre und andere. Sie stellen besondere Anforderungen an die Sicherheit und den Datenschutz, da Daten wie Audio, Video, Desktop usw. über das Internet übertragen werden können und dabei ungewollte, zu viele oder zu sensible Daten übertragen und an Unberechtigte gelangen können. Wie in der Informations-sicherheit bekannt kommt dem Nutzer bzw. seinem Bewusstsein und Können eine große Bedeutung zu. Er kann durch seine Einstellung und sein Handeln die Sicherheit und den Datenschutz deutlich beeinflussen, stärken oder schwächen. In diesem Artikel wurden dazu allgemein Aspekte und Handlungsoptionen vorgestellt: Vorab sollte eine Nutzenabwägung erfolgen, d.h. Präsenzalternativen oder reduzierte Funktionen zu nutzen. Weitere Aspekte sind mitdenken, informieren, die Einstellungen, den Rechner und seine Umgebung vorab sicherheitsoptimieren, die Konferenzsoftware nur zur Durchführung aktivieren und sich auf deren grundlegenden Konferenzfunktionen fokussieren, dazu die Übertragung(en) gezielt nach Bedarf steuern und die übertragenen Daten minimieren und keine schützenswerten Informationen preisgeben.

Literaturhinweise

Gesellschaft für Datenschutz und Datensicherheit e.V.:
GDD-Praxishilfe DS-GVO XVI -Videokonferenzen und Datenschutz, Stand April 2020; www.gdd.de

Bundesamt für Sicherheit in der Informationstechnik:
Kompendium Videokonferenzsysteme (KoViKo - Version 1.0.1), Stand April 2020, www.bsi.bund.de

Firma: DresPleier GmbH ; **Geschäftsführer:** Dr. Christoph Pleier ; **Sitz und Registergericht:** Landshut HRB 6587 ; **USt-ID:** DE814347435
Anschrift: Vils 8, 84149 Velden ; **Telefon:** 08742/5870894 ; **Telefax:** 03222/4170655 ; **Mail:** info@DresPleier.de ; **Web:** www.DresPleier.de