reventix
einfach. clever. verbunden.

Sichere Videokonferenzen

Worauf bei der Wahl des richtigen Anbieters zu achten ist

Inhalt

Sicherheitslücken kosten Unternehmen Milliarden Euro

2019 war jedes Unternehmen von durchschnittlich 206 Cyber-Attacken betroffen, von denen 30 alle Sicherheitsmechanismen überwinden konnten. Angriffe durch Cyberattacken verursachen deutschen Unternehmen jährlich Schäden in Höhe von 43 Mrd. Euro.

Videokonferenzen werden ein immer wichtigerer Teil der Arbeitswelt. Da immer mehr Menschen im Home Office arbeiten und viele Mitarbeiter bereits heute auf Flugreisen zu Geschäftstreffen verzichten, rückt das Thema Videokonferenzen zunehmend in den Fokus. Doch auch Videokonferenzen können ein Einfallstor für Schadsoftware darstellen. Insbesondere, wenn Sie für die Videokonferenz Software auf Ihrem Endgerät installieren müssen.

Wer nun denkt, dass er mit einem namhaften Videokonferenz-Anbieter immer auf der sicheren Seite ist, liegt leider falsch. Das zeigte nicht zuletzt der Fall eines großen amerikanischen Videokonferenz-Anbieters, bei dem sich Hacker Zugriff auf Videokonferenzen und sensible Daten der Teilnehmer verschafft haben. Denn für die Sicherheit von Videokonferenzen ist ein großer Name keine Garantie.

Vielmehr gibt es zahlreiche Kriterien, nach denen Sie die Sicherheit Ihres Videokonferenz-Anbieters beurteilen können. Denn schließlich sind es Ihre Daten und Sie sollten darüber entscheiden, was mit ihnen passiert.

Milliarden €
Schäden durch Cyber-Attacken in Deutschland[1]

Sicherheits-verletzungen pro Jahr in Unternehmen[2]

Durchschnittliche Cyber-Attacken in Unternehmen in 2019[3]

Quelle: 1 Branchenverband Bitkom, 2017 und 2018; 2 https://www.computerwoche.de/a/cyber-angriffe-haben-sich-mehr-als-verdoppelt,3546370; 3 Accenture State of Cyber Resilience report 2019

Sie allein entscheiden über Ihre Daten

Es sind Ihre Daten, also sollten Sie darüber entscheiden, was mit ihnen passiert. Dazu gehört auch, dass Ihre Daten nicht an Dritte weitergegeben werden. Doch was geschieht mit Ihren Daten, wenn Sie einen Anbieter außerhalb der EU nutzen?

Videoanbieter gibt es zahlreiche. Viele große Unternehmen aus diesem Bereich haben Ihren Sitz aber auf dem US-amerikanischen Markt. Für die Sicherheit Ihrer Daten bei einem US-amerikanischen Unternehmen hat bislang der EU-US Privacy Shield gesorgt. Dieser regelte den Schutz personenbezogener Daten, die aus einem Mitgliedsstaat der Europäischen Union in die USA übertragen werden. Doch der Privacy Shield wurde für ungültig erklärt. Was bedeutet das für Ihre Daten? Mit dem Kippen des Privacy Shield verlieren Sie, als Nutzer, auch die Garantie, dass Ihre Daten nicht an Dritte weitergegeben oder gar verkauft werden.

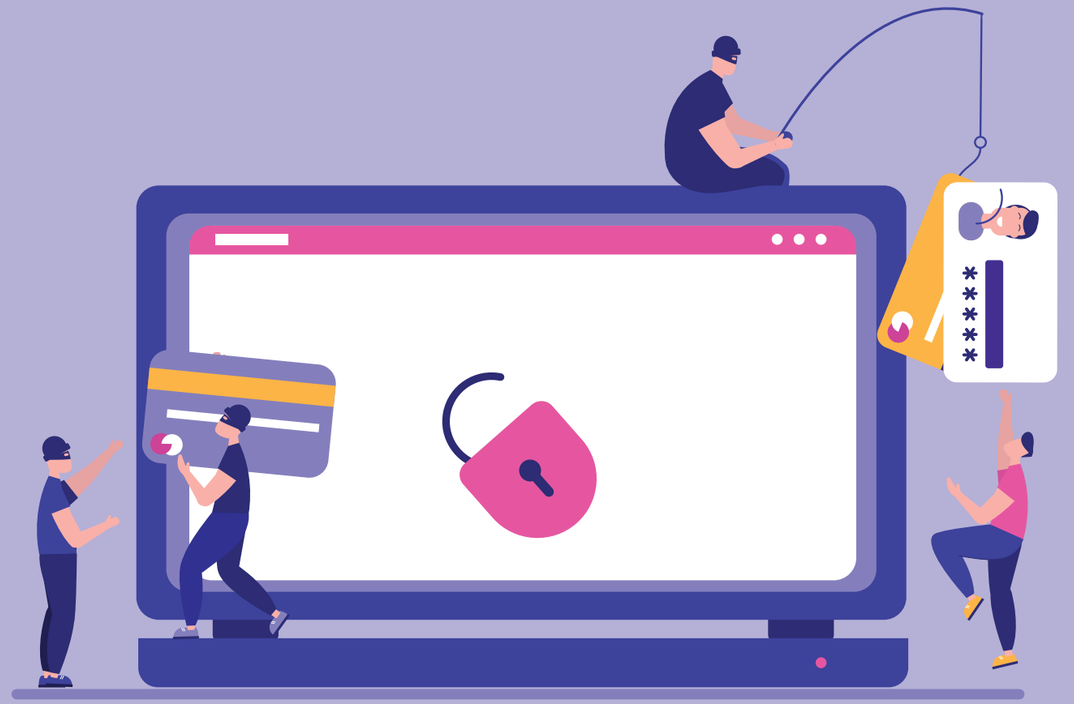
In Deutschland unterliegen alle Ihre Daten der Datenschutzgrundverordnung (DSGVO). Zusätzlich haben Sie die Möglichkeit mit Ihrem Anbieter einen Auftragsverarbeitungsvertrag (AV) zu schließen. Der Auftragsverarbeitungvertrag regelt die Pflichten des verarbeitenden Unternehmen. Ihr Anbieter legt Ihnen beispielsweise offen, wie er Ihre Daten verarbeitet und an welche Dritten er diese ggf. weitergibt. Für unsere Videoplattform reventix rooms nutzen wir keine Software Dritter und geben Ihre Daten daher nicht an andere Unternehmen weiter.

Sicherheitslücke Softwareinstallation

Bei der Wahl eines Anbieters für Videokonferenzen müssen Sie in der Regel zwischen einer browserbasierten und einer Desktop-gestützten Variante wählen. Wir erklären Ihnen warum eine browserbasierte Videokonferenzlösung sicherer als eine Desktop-Anwendung ist.

Sie kennen es sicher. Sie wurden von einem Geschäftspartner zu einem Videomeeting eingeladen. Doch bevor Sie starten können, müssen Sie Software auf Ihren Rechner oder ihr Smartphone herunterladen, um überhaupt teilnehmen zu können. Das ist zum einen nicht nur nervig, wenn Sie verschiedene Partner haben, die alle andere Tools nutzen, sondern auch ein Sicherheitsrisiko. Denn alle Programme oder Apps, die Sie installieren sind potenzielle Gefahren für die Sicherheit Ihrer Daten. So wurde zum Beispiel ein Fall bekannt, in dem mit der Installation der Software eines Anbieters die Gefahr bestand, dass die Steuerung von Webcams und anderen Anwendungen ohne Zustimmung der Nutzer übernommen werden konnte.

Das Problem einer Desktop-Anwendung besteht vor allem darin, dass Sie dem Softwareanbieter voll und ganz vertrauen müssen. Das gibt Ihnen jedoch keinerlei Sicherheit, was er in der Anwendung implementiert hat und wie er mit Ihrem Gerät interagiert. Darüber hinaus kann eine Desktop-Anwendung, wie bereits beschrieben, möglicherweise mehr Schaden an Ihrem Betriebssystem anrichten als Webanwendungen, die in Ihrem Browserfenster isoliert ausgeführt werden. Nutzen Sie deshalb einen Anbieter, dessen Videokonferenz-Plattform browserbasiert ist. In dieser Variante müssen Sie keine Software auf Ihrem Endgerät installieren und bieten Schadsoftware und Hackern somit kein Einfallstor auf Ihren Rechner.



Sicherer Zugang zur Videokonferenz

Kennen Sie “Zoom-Bombing”? So heißt das Phänomen, bei dem sich Unbefugte durch das Erraten von Meeting-IDs in laufende Konferenzen einklinken und unerwünschte Inhalte einfügen. Nun stellen Sie sich das einmal in einer Videokonferenz mit potenziellen Kunden vor.

Nutzen Sie niemals Videokonferenz-Systeme, bei denen ein Link zum Betreten des Konferenzraumes genügt. Zum einen ist ein Link schnell an die falsche Stelle kopiert und zum anderen lässt er sich schnell hacken. So wurden in der Vergangenheit nicht nur Businessmeetings mit unerwünschtem und teils verstörendem Inhalt “gebombt”, sondern es hat auch Online-Gottesdienste und sogar Schulklassen getroffen. Prüfen Sie daher, dass Sie nicht nur über einen öffentlichen Link Zugang zu einer Videokonferenz bekommen, sondern sich immer mit einem Benutzernamen und einem Passwort authentifizieren müssen. So stellen Sie sicher, dass nur autorisierte Personen Zugang zum Meeting haben. Denn hier gilt, je mehr Hürden Sie überwinden müssen, um an dem Meeting teilnehmen zu können, müssen es Hacker auch.

Bei reventix rooms ist ein Passwort verpflichtend. Sie haben auch die Möglichkeit, selbst ein Passwort zu vergeben. Sollten Sie das doch einmal vergessen, generiert unser Sytsem automatisch ein Passwort für Sie. Hier gilt das Motto: Ohne Passwort keine Konferenz. Zusätzlich können Sie für Teilnehmer und Moderatoren verschiedene Passwörter vergeben, die darüber auch verschiedene Rechte erhalten.

Sichere Kommunikation durch Verschlüsselung

So wichtig sichere Kommunikation beim Telefonieren oder Chatten ist, so wichtig ist sie auch bei Videokonferenzen. Dazu zählt nicht nur die Vergabe von Passwörtern, sondern auch was Ihr Anbieter im Hintergrund für die Sicherheit Ihrer Kommunikation tut.

In Videokonferenzen teilen wir genauso sensible Daten oder Inhalte wie im Internet. Ist es dort die PIN zum Online-Bankkonto, sind es bei der Videokonferenz sensible Inhalte und Teilnehmerdaten. Personal-Firewall- und Anti-Malware-Lösungen auf lokalen Computern bieten hierbei keinen Schutz. Achten Sie deshalb auf eine verschlüsselte Kommunikation via TLS/SSL auch bei Ihrem Videokonferenz-Anbieter. Die Kommunikation in reventix rooms läuft gesichert via HTTPS zwischen Endgeräten und den Servern. Dabei nutzen wir selbstverständlich die Verschlüsselung mit TLS/SSL nach neustem Standard. Da reventix rooms eine rein browserbasierte Konferenz-Plattform ist, müssen Sie keinerlei Einstellungen an Ihrer Firewall vornehmen. Zudem ist es eine Eigenentwicklung, die auf dem Open Source-Projekt BigBlueButton beruht. Das bietet den Vorteil, dass der Quellcode komplett einsehbar ist und regelmäßig von einer großen Gruppe von Entwicklern weiterentwickelt und gepflegt wird. So ist es zum Beispiel dauerhaft sicher vor Manipulationen Dritter oder Hintertüren, sogenannten Backdoors, mit denen der gesicherte Zugang umgangen werden kann. Damit gehört BigBlueButton zu den sichersten Webkonferenzsystemen weltweit.

Rechte von Konferenzteilnehmern vorab festlegen

Sie kennen es sicher: Sie treten in eine Videokonferenz ein und bei einem Teilnehmer brummt die Kaffeemaschine, beim nächsten bellt ein Hund. Vielleicht hat aber auch schon ein Teilnehmer seinen Bildschirm geteilt, auf dem die Übersicht seines Online-Bankingkontos zu sehen ist.

In jeder Videokonferenz-Plattform haben sowohl Teilnehmer als auch Moderatoren bzw. Gastgeber verschiedene Rechte. Sei es das Mikrofon, die Übertragung der Webcam oder das Teilen des Bildschirms. Werden Rechte von Teilnehmern nicht eingeschränkt, kann das zu einem großen Sicherheits-Fauxpas führen, wie zum Beispiel das ungewollte Zeigen von internen Unterlagen und Ordnern auf dem Desktop. Solche Rechte Ihrer Teilnehmer können Sie nicht nur, sondern sollten Sie von vornherein einschränken.

Neben dem Mikrofon und der Webcam gibt es weitere Rechte, die Sie bereits vor dem Meeting einschränken können. So haben Sie bei reventix rooms die Möglichkeit, Teilnehmer für andere Teilnehmer unsichtbar zu machen. Das ist vor allem wichtig, wenn Sie Konferenzen abhalten, die Sie aufzeichnen und im Anschluss gegebenenfalls im Internet verbreiten. So sind die Daten Ihrer Teilnehmer vor den Augen anderer geschützt.

Sie können aber auch generell das Nutzen der Webcam verbieten oder einstellen, dass nur Sie, als Moderator, die Stummschaltung der Teilnehmer aktivieren und deaktivieren. Auch können Sie das Verbreiten unerwünschter Informationen unterbinden, indem Sie den Teilnehmern von vornherein die Nutzung des privaten oder öffentlichen Chats verbieten.

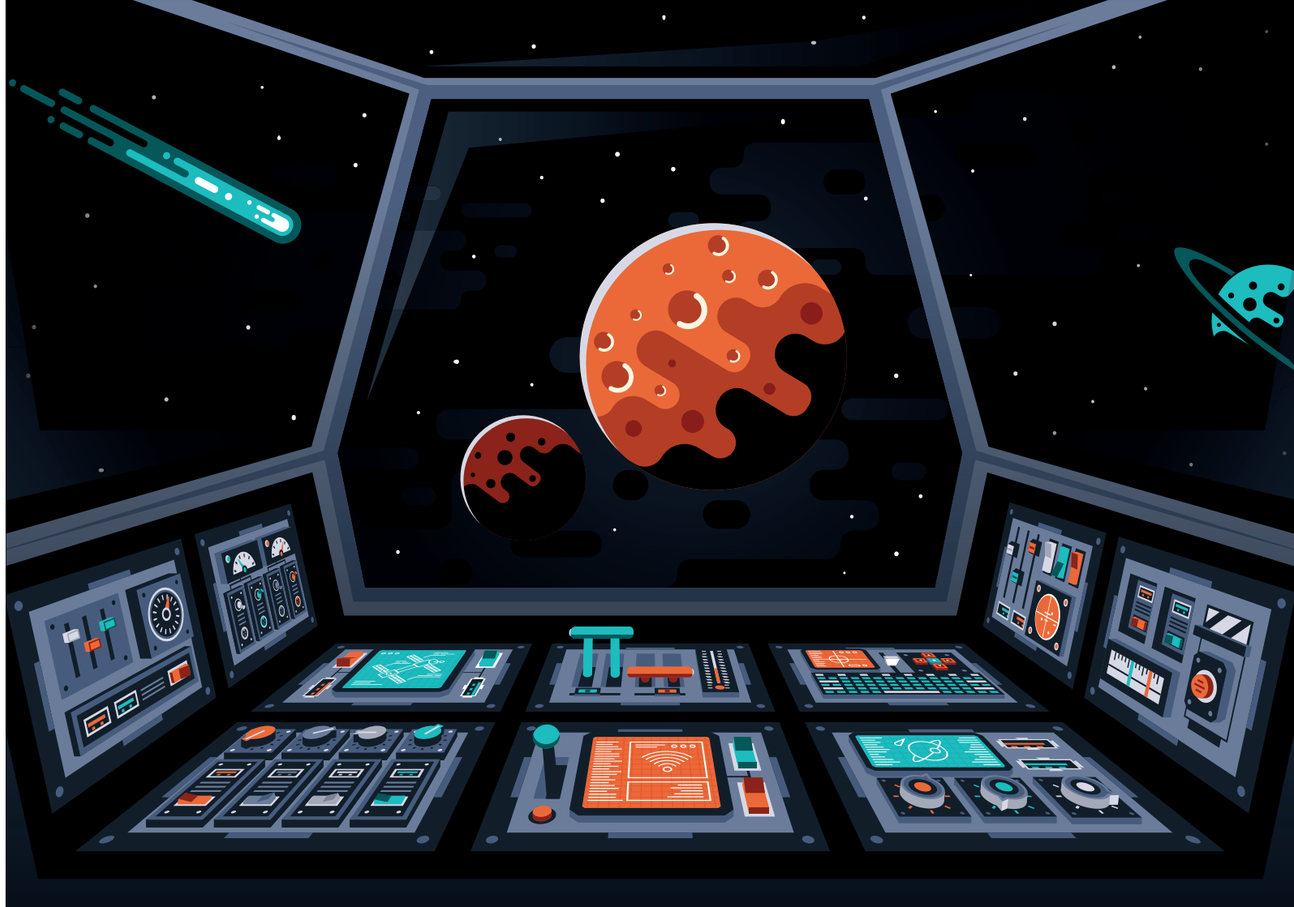
Während der Videokonferenz alles unter Kontrolle

Neben dem vorsorglichen Einschränken von Rechten Ihrer Teilnehmer, sollten Sie auch während einer Konferenz volle Kontrolle haben und Ihren Teilnehmern jederzeit Rechte geben und wieder entziehen können.

Stellen Sie bei der Wahl des Anbieters sicher, dass Sie auch während eines Videomeetings volle Kontrolle behalten. Das beginnt bereits beim Teilen des Bildschirms. Hier sollten Sie darauf achten, dass Sie nicht nur Ihren gesamten Desktop teilen könne, sondern auch zwischen Anwendungsfenstern und Browserfenstern entscheiden können. Bei vielen Anbietern, können Sie auch nur einen Tab des Browsers teilen. So stellen Sie sicher, dass niemand sensible Daten sehen kann, die Sie eventuell in einem Programm geöffnet oder in einem Ordner abgelegt haben.

In Videokonferenzen kommt es auch oft vor, dass neben dem Moderator auch ein Teilnehmer etwas zeigen möchte. Hier sollten Sie darauf achten, dass kein Teilnehmer einfach die Kontrolle übernehmen kann. Weder auf Ihren geteilten Inhalt, noch, dass er selbst etwas teilen kann. Prüfen Sie immer, dass Sie ihm zuerst das Recht geben müssen, etwas zu teilen und ihm das Recht genauso schnell wieder entziehen können.

Auch beim gemeinsamen Brainstorming und Ideensammeln am interaktiven Whiteboard sollten Sie die Rechte der Teilnehmer aktiv zuweisen und auch wieder entziehen dürfen. Mit unserer Videokonferenz-Plattform können Sie andere Teilnehmer unkompliziert zum Präsentator machen, ihnen dieses Recht aber mit nur einem Klick auch wieder nehmen.



Serverstandort Deutschland garantiert Sicherheit

„Made in Germany“ ist nicht nur bei der Wahl von Produkten ein Qualitätsmerkmal, sondern auch in Sachen Serverstandort, denn deutsche Anbieter unterliegen dem strengen deutschen Datenschutzgesetz und – damit verbunden – umfassenden Sicherheitsvorkehrungen.

Was den Schutz persönlicher Daten betrifft, ist das deutsche Recht eines der strengsten weltweit. Dabei ist nicht nur maßgeblich in welchem Land ein Unternehmen seinen Hauptsitz hat, sondern auch, in welchem Land sich die Server befinden. Hat zum Beispiel ein Unternehmen zwar seinen Hauptsitz in Deutschland, aber seine Server und eine Niederlassung in einem anderen Land, gilt das Recht des Niederlassungslandes. Deshalb ist auch der Serverstandort Deutschland für Kunden essentiell.

Darüber hinaus ist der Serverstandort auch für die geltenden Eingriffsrechte wichtig: Dazu zählen Überwachungsmaßnahmen und Anordnungen auf die Herausgabe von Daten an Behörden wie die Polizei. Nur Unternehmen, die neben dem deutschen Hauptsitz ihren Serverstandort ebenfalls in Deutschland haben, unterliegen bei solchen Eingriffsrechten dem deutschen Recht. Deshalb sollten Sie Anbieter wählen, deren Server sich in Deutschland in zertifizierten Rechenzentren befinden und deswegen strengen Sicherheitsstandards unterliegen.

5 Tipps für eine sichere Videokonferenz

Passwort verpflichtend

Ohne Passwort sollten Sie keine Konferenz erstellen oder an einer teilnehmen.

Serverstandort Deutschland

Achten Sie darauf, dass Ihr Anbieter Server in deutschen Rechenzentren betreibt, denn sie gelten als die sichersten weltweit.

Verschlüsselung

Stellen Sie sicher, dass Ihre Kommunikation via Videokonferenz immer verschlüsselt erfolgt.

Immer browserbasiert

Ziehen Sie eine Konferenz in Ihrem Internetbrowser immer einer Konferenz vor, bei der Sie ein Programm installieren müssen.

Rechte vergeben

Stellen Sie sicher, dass Sie Ihren Teilnehmern jederzeit Rechte geben und wieder entziehen können.

reventix
einfach. clever. verbunden.

Ihr Firmenstempel

www.reventix.de

reventix GmbH • Landhausstr. 22 • 10717 Berlin