Datenschutz *aktuell - Ausgabe 01-2022*

Der Datenschutz-Newsletter aus Nürnberg

Liebe Leserin,
lieber Leser,

die Welt wird derzeit von mehreren Krisen heimgesucht. Erst die Corona Pandemie und nunmehr der Krieg in der Ukraine verändern unser altgewohntes Weltbild.

Auch unser Wirtschaftsleben hat sich gewandelt. Schulungen werden neben der Präsenz online durchgeführt, Beratungen finden ebenfalls teilweise vor dem Bildschirm statt. Gerade in diesen Bereichen ist es wichtig, auch das Thema Datenschutz auf der Agenda zu haben.

Anbei finden Sie wieder eine Auswahl von Themen zu Ihrer Information. Natürlich stehe ich Ihnen auch gerne persönlich für Auskünfte zur Verfügung.

Mit den besten Grüßen aus Nürnberg

Peter Brandmann
(Externer Datenschutzbeauftragter)

Aufgepasst bei Online-Videokonferenzen!

Statt persönlicher Besprechungen vor Ort finden vermehrt Videokonferenzen über das Internet statt. Viele dieser Online-Services sind leicht zu bedienen, so scheint es. In Wirklichkeit aber gibt es einiges zu beachten, damit Ihre Privatsphäre geschützt bleibt.

Live aus dem Homeoffice

Unter dem Eindruck der Coronakrise hat sich das Arbeiten in vielen Branchen verändert. 95 Prozent der Unternehmen ersetzen Präsenztreffen durch Videokonferenzen, so eine Umfrage des Digitalverbands Bitkom. Wenn Sie gegenwärtig auch im Homeoffice arbeiten, kennen Sie sicherlich die beliebten Videokonferenz-Dienste wie Zoom oder Teams.

Für die Durchführung von Online-Besprechungen oder die Teilnahme daran ist kaum eine Installation erforderlich. Browser, Webcam, Mikrofon, Lautsprecher und gute Internetverbindung reichen. Entsprechend oft am Tag nimmt man an einem der Online-Meetings teil. Das ist bereits so stark Teil des beruflichen Alltags geworden, dass manche Teilnehmer vergessen, dass die Webcam oder das Mikrofon schon oder noch angeschaltet ist. So werden Bilder und Töne übertragen, die eigentlich nicht für die Öffentlichkeit bestimmt waren. Doch die Privatsphäre ist noch stärker in Gefahr.

Datenschützer und Sicherheitsbehörden geben wichtige Hinweise

Die Aufsichtsbehörden für den Datenschutz haben eine Orientierungshilfe zu Videokonferenzsystemen veröffentlicht und geben darin auch wichtige Hinweise, die die Nutzerinnen und Nutzer betreffen. Daraus ergeben sich Punkte, die Sie bei Online-Videokonferenzen beachten sollten.

Zum einen ist es wichtig, nur im Unternehmen freigegebene Dienste zu nutzen, auch dann, wenn Sie im Rahmen Ihrer beruflichen Tätigkeit selbst eine Online-Konferenz planen und dazu einladen.

Zum anderen sollten Sie auf bestimmte technische und organisatorische Maßnahmen achten, um Ihre Privatsphäre besser zu schützen, wie das BSI (Bundesamt für Sicherheit in der Informationstechnik) unterstreicht:

- Stellen Sie sicher, dass nur die Personen an Ihrem Online-Treffen teilnehmen, die Sie auch eingeladen haben – das geht beispielsweise mit einer komplexen PIN für Ihren virtuellen Raum.
- Überschreiben Sie die Standardvorgaben der Raumbezeichnung und Ihrer Nutzerkennung durch individuelle Namen. Achten Sie darauf, dass Sie keine trivialen Passwörter, Nutzerkennungen oder PINs vergeben.
- Geben Sie nur die nötigsten Daten ein, wenn Sie sich für den Dienst registrieren müssen.
- Machen Sie sich bewusst, was Sie zeigen, wenn Sie den Bildschirm teilen. Wenn Sie Daten austauschen, können auch Schadprogramme übertragen werden.
- Schließen Sie Sicherheitslücken, indem Sie Updates installieren.
- Achten Sie darauf, dass im genutzten Webbrowser eine aktive Verschlüsselung bestätigt wird, zum Beispiel in der Adresszeile des Browsers durch „https“.
- Schalten Sie Webcam und Mikrofon nur ein, wenn Sie diese wirklich brauchen, und deaktivieren Sie danach diese Funktionen wieder.
- Nutzen Sie für die Webcam am besten eine Abdeckung, die sich vor- und wegschieben lässt.

Beherzigen Sie diese Sicherheitshinweise, um von sich und Ihrem Homeoffice nicht mehr preiszugeben, als Sie wollen.

Meetings datenschutzkonform organisieren

Wer Meetings organisiert, muss den Datenschutz im Blick haben. Das überrascht viele. Aber manchmal geht es in Meetings um heikle Dinge. Oft spricht man über Personen oder über Dinge, die Personen betreffen. Grund genug, sich einige Gedanken zu machen. Aber auch das „Drumherum“ vor und nach einem Meeting verdient Aufmerksamkeit.

Einladung zum Meeting

Schon bei der Einladung kann einiges schiefgehen. Oft erfolgt die Einladung über eine Rundmail. Sie geht an eine Kontaktgruppe, die im Mail-Adressbuch hinterlegt ist. Der Mail-Verteiler muss dann wirklich noch aktuell sein. Mitarbeiter, die längst an ganz andere Stellen im Unternehmen gewechselt sind, haben darin nichts mehr zu suchen. Nehmen Sie die nächste Einladung per Rundmail also zum Anlass, sich den Verteiler einmal genau anzusehen.

Vorsicht bei „an“, „Cc“ und „Bcc“

Kein Problem ist es beim internen Meeting einer Arbeitsgruppe, wenn alle Adressaten den vollständigen Verteiler sehen können. Er kann dann im Adressfeld „an“ stehen. Denn oft besteht eine wichtige Information gerade darin, wer alles zu dem Meeting eingeladen ist.

Das gilt allerdings nicht immer. Denn Meeting und Meeting ist nicht dasselbe. Wenn etwa die Einladung für eine Personalversammlung an die ganze Belegschaft geht, gehört die Adressliste selbstverständlich in das Feld „bcc“. Dann ist sie für die Adressaten nicht offen sichtbar.

Überlegen Sie also vorher, ob die Adressaten den ganzen Verteiler der Einladung sehen sollen oder nicht.

Doodle oder nicht?

Doodle ist praktisch und sehr beliebt. Es hat aber eine Schwachstelle: Wer auf eine Terminabfrage zugreifen will, muss einen Link aufrufen, den er bekommen hat. Dieser Link darf nicht in unrechte Hände geraten. Darauf muss man unbedingt achten. Denn Daten über Termine sind keineswegs immer so harmlos, wie viele glauben. Wer wann mit wem spricht und wer wann dafür Zeit hat, kann eine sehr interessante Information sein.

Alternativen zu Doodle gibt es durchaus, und zwar kostenlose. Beispiele dafür sind „dudle“ von der Technischen Universität Dresden und der „DFN-Terminplaner“. Beide sind vor allem im Wissenschaftsbereich weit verbreitet. Es handelt sich allerdings um Software, die man auf dem Rechner installieren muss. Das setzt in Unternehmen normalerweise eine entsprechende Genehmigung der EDV voraus. Bitte beachten Sie die Regelungen, die dafür im Unternehmen bestehen!

Teilnehmerlisten bei internen Meetings

Bei einer internen Besprechung etwa zum Thema „Absatzplanung 2021“ kann jeder Teilnehmer eine Teilnehmerliste erhalten. In sie gehören die Namen und die dienstlichen Kommunikationsdaten der Besprechungsteilnehmer. Nur so können sie später noch einmal zuverlässig miteinander Kontakt aufnehmen, wenn das nötig ist. Der Zweck einer solchen Besprechung erfordert es geradezu, dass alle eine Teilnehmerliste erhalten.

Teilnehmerlisten bei Schulungsveranstaltungen

Ganz anders sieht es etwa bei Schulungsveranstaltungen mit externen Teilnehmern aus. Selbstverständlich ist hier eine interne Liste möglich, auf der jeder Teilnehmer unterschreibt. Sie kann Verwendung finden, um Teilnehmerbestätigungen und Rechnungen für die Schulungsgebühren zu erstellen.

Nicht in Ordnung wäre es dagegen, jedem Teilnehmer eine Liste mit allen anderen Teilnehmern auszuhändigen. Das ist normalerweise nicht erforderlich, um das Ziel einer solchen Veranstaltung zu erreichen. Tauschen Teilnehmer ihre Kommunikationsdaten trotzdem untereinander aus, ist es ihre Privatangelegenheit.

Tücken bei Telefonkonferenzen

Telefonkonferenzen gehören inzwischen zum Alltag. Virtuelle Konferenzräume dafür gibt es im Internet kostenlos. Achten Sie aber einmal darauf, was Ihr Lieblingsanbieter zum Thema Datenschutz sagt. Gar nichts? Dann existiert bei ihm Datenschutz wahrscheinlich auch nicht.

Wichtig ist vor allem: Lässt sich der Konferenzraum „abriegeln“, wenn ihn alle Teilnehmer betreten haben? Sonst besteht die Gefahr, dass sich Unbefugte einklinken und mithören. Generell sollte man darauf achten, dass der Konferenzanbieter ein Sicherheitszertifikat einer anerkannten Organisation vorzuweisen hat. Dann dürften zumindest keine groben Schwachstellen vorhanden sein.

Videokonferenz – aber sicher!

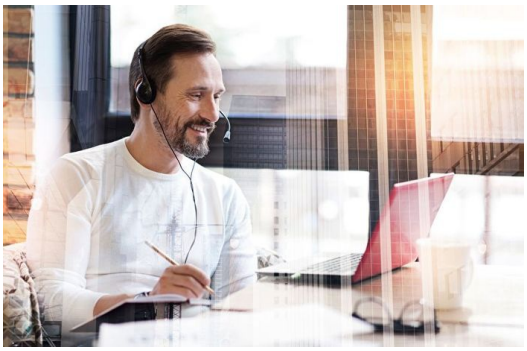
Sicherheit kann ein sehr trügerisches Gefühl sein. Wer an einer Videokonferenz teilnimmt, meint subjektiv, dass er buchstäblich „alles überblicken“ kann. Aber was ist, wenn sich ein Unbefugter einklinkt und unbemerkt die ganze Konferenz verfolgt? Hier kommt das Thema „Verschlüsselung“ ins Spiel.

Verschlüsselung ist nicht gleich Verschlüsselung

Manche Anbieter setzen eine „Ende-zu-Ende-Verschlüsselung“ ein. Bei ihr können nur die Teilnehmer der Konferenz selbst die Daten wahrnehmen, sprich die Bilder sehen und die Sprache hören. Sie bietet mehr Sicherheit als

eine reine „Transportverschlüsselung“. Bei dieser ist es zumindest technisch möglich, dass „Datentransporteure“, die für die Übermittlung der Daten sorgen, die Daten entschlüsseln. Damit stellt sich die Frage, ob man sich mit weniger zufriedengeben soll, wenn man auch mehr Sicherheit haben kann. Dafür gibt es keine allgemein verbindlichen Vorgaben der Datenschutz-Aufsichtsbehörden. Anlass zum Nachdenken besteht aber allemal.

Videokonferenzen im Fokus von Cyberattacken



Die Zahl der beruflichen und privaten Videokonferenzen hat stark zugenommen. Das weckt das Interesse der Datendiebe. Ohne die erforderlichen Sicherheitsmaßnahmen ist die Vertraulichkeit der Gespräche und ausgetauschten Daten in Gefahr.

Der Berufsalltag wandelt sich

Wissenschaftler gehen davon aus, dass die Corona-Pandemie die Arbeitswelt auch längerfristig verändert. Im Arbeitsalltag werden wohl häufiger virtuelle Treffen anstelle von Konferenzen vor Ort stattfinden.

Leider fehlt vielen Berufstätigen noch die Erfahrung, um Videokonferenzen sicher nutzen zu können. Dadurch gerät der Datenschutz in Gefahr.

Videokonferenzen bergen viele Risiken

Marit Hansen, die Landesbeauftragte für Datenschutz Schleswig-Holstein, betont: „Da Videokonferenzen für viele neu sind, haben nicht alle im Blick, welche Risiken damit verbunden sind. Gerade in der Kombination mit Homeoffice ist einiges zu beachten. Um die Teilnehmenden von Videokonferenzen und die besprochenen Inhalte zu schützen, sind technische und organisatorische Sicherheitsmaßnahmen wichtig.“

IT-Sicherheitsexperten warnen davor, dass zum Beispiel ein ungebetener Gast an einer Videokonferenzsitzung teilnehmen könnte, um entweder das Gespräch mitzuhören oder die Sitzung durch den Austausch ungeeigneter Medien zu stören. Ebenso könnten Meeting-Links und -Zugänge gestohlen sowie bösartige Links und Schadsoftware verteilt werden.

Im Juni 2020 warnte zum Beispiel das Bundesamt für Sicherheit in der Informationstechnik (BSI), dass Angreifer mehrere Schwachstellen in Zoom Video Communications ausnutzen konnten, um Schadcode auszuführen. Unter anderem konnte dies mittels speziell manipulierter animierter Bilddateien geschehen. Für einen Angriff genügte es, die vom Angreifer versendete Datei im Chat empfangen zu haben. Die Datei musste nicht extra geöffnet werden.

Auf eine sichere Lösung kommt es an

Die Aufsichtsbehörden für den Datenschutz warnten in den letzten Monaten vor verschiedenen Lösungen für Videokonferenzen, weil personenbezogene Daten in Gefahr geraten konnten, und empfahlen datenschutzfreundlichere Alternativen.

Die Berliner Beauftragte für den Datenschutz zum Beispiel empfiehlt, zu prüfen,

- ob anstelle von Videokonferenzen auch Telefonkonferenzen ausreichen könnten, um die gewünschte Abstimmung untereinander herbeizuführen,
- ob es mit verhältnismäßigem Aufwand möglich ist, einen eigenen Dienst für Videokonferenzen mit öffentlich verfügbarer oder kommerziell erhältlicher Software bereitzustellen, und
- ob Lösungen eines Anbieters mit Sitz und Verarbeitungsort, insbesondere Server-Standort, im Europäi-

schen Wirtschaftsraum (EWR) oder aus einem Land mit gleichwertigem Datenschutzniveau den Bedürfnissen des jeweiligen Unternehmens entsprechen.

Der gewählte Anbieter sollte die Daten nur im zulässigen Rahmen verarbeiten und insbesondere nicht entgegen europäischem Datenschutzrecht an Dritte – einschließlich ausländischer Behörden – weitergeben, ausreichende Datensicherheit (zum Beispiel durch Zertifizierung) nachweisen können, die Verschlüsselung der Datenübertragung garantieren und einen ordnungsgemäßen Auftragsverarbeitungsvertrag anbieten.

Auch wichtig: das richtige Verhalten der Teilnehmerinnen und Teilnehmer

Allein die Wahl einer datenschutzgerechten Lösung reicht aber nicht, sie muss auch genutzt werden: Laut einer Kaspersky-Studie verwenden 26 Prozent der deutschen Mitarbeiter nicht genehmigte Videokonferenz-Tools und setzen die eigenen Daten und die Daten des Arbeitgebers möglichen Angriffen aus. Security-Experten beobachten den Trend, der BYOM (Bring Your own Meeting) genannt wird, also die Verwendung privater Videokonferenz-Lösungen zu betrieblichen Zwecken. Das kann gerade im Home-Office leicht passieren.

Bei den „kostenfreien“ Diensten sollte man ganz genau in die Datenschutzbestimmungen schauen. Oftmals zahlen die Nutzer hier mit ihren Daten. Das kann nicht im Sinne von Unternehmen sein und auch nicht im Sinne des Nutzers selbst.

Für den Datenschutz kommt es deshalb auch auf das Verhalten der Teilnehmer an. Die Datenschutzaufsicht von Schleswig-Holstein rät den Teilnehmern an Videokonferenzen insbesondere:

- Informieren Sie sich bei der organisierenden Person, ob im Zusammenhang mit der Videokonferenz eine Datenschutzerklärung oder eine Datenschutz-Kurzinformation bereitgestellt wird.
- Testen Sie die Funktionen, mit denen Sie Ihre Privatsphäre schützen können, um sie während der Videokonferenz sicher verwenden zu können, zum Beispiel Ton und/oder Bild deaktivieren.
- Seien Sie sich bewusst, dass in einer Videokonferenz alle anderen Teilnehmenden zuhören, und geben Sie keine sensiblen Informationen weiter.

- Schalten Sie Ihr Mikrofon stumm und ggf. die Kamera aus, etwa wenn im Homeoffice andere Personen aus Ihrem Haushalt in den Aufnahmebereich des Mikrofons oder in das Sichtfeld der Kamera kommen.
- Seien Sie in der Videokonferenz aufmerksam und informieren Sie die organisierende Person bzw. die anderen Teilnehmenden, wenn beispielsweise eine fremde Person den Konferenzraum betritt.

Impressum
Redaktion: Peter Brandmann (V.i.S.d.P.)
Externer Datenschutzbeauftragter - Zert. Fachkraft DSGVO
Anschrift:
pb beratung & training
Schnepfenreuther Weg 51
90425 Nürnberg

Telefon: 0911/3506118
E-Mail: peter.brandmann@pb-beratung-training.de