2020/23 Inland

https://shop.jungle.world/artikel/2020/23/ungesichert-die-konferenz

Die Berliner Datenschutzbehörde hat Ärger mit Microsoft

Ungesichert in die Konferenz

Von **Boris Mayer Elke Wittich**

Die Berliner Datenschutzbehörde hat auf Sicherheitsmängel bei Anbietern von Videokonferenzen aufmerksam gemacht. Microsoft protestiert gegen die namentliche Nennung.

Besonders durchdacht wirkt das Vorgehen der Berliner Datenschutzbehörde nicht: Zunächst veröffentlichte sie Empfehlungen für Videokonferenzen. Einige Tage später nahm sie die Dokumente wieder von ihrer Website, um sie dann, knapp zwei Wochen später, mit nur kleinen Änderungen erneut zu veröffentlichen.

Datenschutz ist ein wichtiges Thema – auch wenn die gesetzlichen Regelungen für die Betreiber Aufwand erzeugen und die Benutzer manchmal nerven, weil niemand gerne auf jeder benutzten Website die Datenschutzerklärung über die Verwendung von Cookies und Verkehrsdaten durchklickt. Es ist auch wichtig zu verhindern, dass Firmen auf ihren Websites gesammelte personenbezogene Daten kommerziell verwerten, ohne dass der betroffene Nutzer dem zugestimmt hätte. Deswegen wäre es angebracht, dass eine mit dem Thema beauftragte Behörde ihre Empfehlungen verständlich, aktuell und mit der nötigen Rechtssicherheit ausspricht, um User nicht weiter zu verunsichern – gerade in Zeiten, in denen Verschwörungstheoretiker fast alles als *fake news* deklarieren. Selbstverständlich wäre eine klare Kommunikation auch gut, um den Datenschutz nicht im Zuge einer Provinzposse der Lächerlichkeit preiszugeben. Aber man kann halt nicht alles haben.

> Empfehlungen von Datenschutzbehörden, wie man sicher mit Videokonferenzen arbeitet, helfen Nutzern einen Monat nach dem Beginn der Zeit im Homeoffice kaum.

Was genau war passiert? Der Grund für die Depublikation und die spätere Neuveröffentlichung war eine kleine Passage in dem Dokument. »Wir weisen darauf hin, dass einige verbreitet eingesetzte Anbieter die aufgeführten Bedingungen nicht erfüllen, darunter Microsoft, Skype Communications und Zoom Video Communications«, hieß es dort. Microsoft störte sich an der Nennung, forderte ein Gespräch und schrieb einen Brief, der am 11. Mai bei der Behörde eintraf. Daraufhin nahm diese das Dokument aus dem Netz, erklärte, dass man dies ohne Prüfung des Sachverhalts vorsorglich getan habe, und veröffentlicht es elf Tage später, am 22. Mai, erneut, versehen mit dem Hinweis: »Die Überprüfung der Dokumente durch die Berliner

Aufsichtsbehörde hat keinen inhaltlichen Änderungsbedarf der Empfehlungen ergeben, es wurden nur einige geringfügige Konkretisierungen an den Texten vorgenommen.«

Dass Microsoft nicht begeistert war und versucht, gegen die Erwähnung vorzugehen, verwundert nicht, zumal der Konzern bei den drei beispielhaft genannten Unternehmen gleich zweimal vertreten ist, denn Skype gehört Microsoft. Das hätte auch die Behörde nicht weiter erstaunen sollen. Zudem steigert die explizite Nennung der drei Firmen die Aussagekraft des Dokuments nicht. Selbst nach dem Eintreffen des Briefs von Microsoft hätte die Behörde die betreffende Passage einfach streichen und die Empfehlungen online verfügbar lassen können.

Der Einsatz von Software für Videokonferenzen geht notwendig mit Unsicherheit einher, nicht nur den Datenschutz betreffend. Denn solange man einen externen Dienst verwendet, um Videokonferenzen technisch zu betreiben, landen Videos der Teilnehmer beim Betreiber auf den Servern, werden dort verarbeitet, miteinander verknüpft und als Ganzes wieder an die Teilnehmer der Konferenz zurückgeschickt. Verschlüsselung ist dabei nur auf den Transportwegen üblich, also vom Teilnehmer zum Server des Betreibers und zurück. Ende-zu-Ende-Verschlüsselung ist bei mehr als zwei Teilnehmern technisch schwer herzustellen, denn dann müsste jeder Teilnehmer sein Video und Audio einzeln an jeden anderen Teilnehmer streamen. Dazu benötigte jeder Teilnehmer nicht nur ein Vielfaches seiner üblichen benutzten Bandbreite, sondern auch einen Computer, der gleichzeitig einen Videostream kodieren und verschlüsseln sowie andere Videostreams entschlüsseln, dekodieren und anzeigen kann. WebRTC (Web Real-Time Communication, Netzechtzeitkommunikation), der Standard für sichere Kommunikation im Browser, unterstützt nur die Verbindung zwischen zwei Endpunkten, also entweder zwischen zwei Teilnehmern oder einem Teilnehmer und einem Server.

Doch das sind nicht einmal alle Probleme, die gelöst werden müssten, um eine sichere Verschlüsselung zu ermöglichen, bei der der Anbieter keine Einblicke erhält. Sobald der Dienst auch die Einwahl per Telefon umfasst, muss er die Möglichkeit zum Entschlüsseln haben, um das Gesagte in die Telefonleitung einspeisen zu können. Gleiches gilt für Mitschnitte, automatische Übersetzungen und vieles mehr. Wer nicht mithören kann, kann auch nichts abspeichern, übersetzen oder in ein anderes Medium überführen.

Allerdings sind der ungeschickte Umgang mit der Nennung einiger Firmen und die Reaktion auf die Kritik von Microsoft gar nicht das Schlimmste. Unglücklicher ist das Timing: Die Empfehlungen kamen viel zu spät. Videokonferenzen gibt es schon seit einigen Jahren, aber durch die Pandemie und die damit verbundenen Beschränkungen hat sich ihre Nutzung in Unternehmen und Behörden sprunghaft ausgeweitet. Empfehlungen von Datenschutzbehörden, wie man sicher mit Videokonferenzen arbeitet, helfen Nutzern einen Monat nach dem Beginn der Zeit im Homeoffice kaum. Mit den Berliner Empfehlungen verhält es sich wie mit einem vor Stunden bestellten Taxi, das vorfährt, wenn der zu erreichende Zug schon den Bahnhof verlassen hat.