Der Landesbeauftragte für den
Datenschutz Niedersachsen

Technische Eckpunkte für den Einsatz von Videokonferenzsystemen in Schulen (Mai 2021)

Die Eckpunkte beziehen sich auf die zentralen Aspekte des technischen und organisatorischen Datenschutzes und die damit verbundenen Maßnahmen (TOM), die an alle Videokonferenzsysteme (VKS) zu stellen sind. Eine detailliertere Hilfestellung zu den datenschutzrechtlichen Anforderungen an ein VKS bieten die FAQ der LfD Niedersachsen und die Orientierungshilfe mit Checkliste der DSK.

Anwendungsbereiche individuell prüfen

Es wird im schulischen Umfeld viele Abläufe und Anforderungen geben, die sich standardisiert behandeln lassen. Das ist auch ein Grund, warum eine landesweit einheitliche Infrastruktur und Anwendungslandschaft (z. B. Schul- oder Bildungscloud) sinnvoll erscheint. Gleichwohl bedarf es der Einzelfallbetrachtung der Anwendungsbereiche der einzelnen Schule, die teils Unterschiede bei den Daten, Prozessabläufen (Anwendungskontext) und der eingesetzten Hard- und Softwarekomponenten aufweisen können. Diese Unterschiede bedürfen einer individuellen Prüfung bei der Risikobewertung und der notwendigen Ermittlung der geeigneten technischen und organisatorischen Datenschutzmaßnahmen, um ein angemessenes Schutzniveau zu erreichen.

- Wie diese Prüfung methodisch Schritt für Schritt ablaufen sollte, hat die LfD Niedersachsen in ihrer Handlungsempfehlung ZAWAS veröffentlicht, deren Beachtung hier empfohlen wird.
- Wenn datenschutzrechtliche Anforderungen inkl. TOM erfüllt werden sollen, muss geprüft werden, ob dies in Eigenregie vom Schulträger (Eigenbetrieb) bzw. von einem Dienstleister (Auftragsverarbeiter) in einer eigenen Instanz geleistet wird. Auftragsverarbeiter können sich auch weiterer Auftragsverarbeiter bedienen (insbesondere bei Cloud-Dienstleistungen). Unterauftragsverarbeitungsverhältnisse bedürfen jedoch der vorherigen Genehmigung durch den Verantwortlichen (Schule). Falls diese Anforderungen nicht bereits erfüllt werden, sind ggf. Anpassungen der Software notwendig.

Mindeststandard: Transportverschlüsselung

Die Datenübermittlungen benötigen Schutz auf der Übertragungsstrecke bis zum Provider. Bei der Übertragung der Videokonferenzdaten muss mindestens eine Transportverschlüsselung nach dem Stand der Technik, entsprechend dem einschlägigen Kompendium des Bundesamts für Sicherheit in der Informationstechnik (BSI) für VK-Systeme und den Technischen Richtlinien des BSI (siehe Ausführungen der FAQ der LfD Niedersachsen) implementiert sein. Damit ist jedoch noch nicht sichergestellt, dass alle beteiligten Teilabschnitte des Netzes bis zu allen VK-Teilnehmenden vor unbefugter Kenntnisnahme geschützt sind.

Ende-zu-Ende-Verschlüsselung

Wenn die Risiko basierte Prüfung zur Sicherheit der Verarbeitung gem. Art. 32 Abs. 1 DS-GVO und unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung, ergibt, dass die Gewährleistungsziele Vertraulichkeit oder Integrität eine Ende-zu-Ende-Verschlüsselung (E2EE) als geeignete technische und organisatorische Maßnahme erfordert, dann muss dabei beachtet werden:

- Für den Fall, dass das VKS bereits als Produkt eine E2EE anbieten würde, muss gewährleistet sein, dass der Anbieter diese auch implementiert haben (z. B. SRTP, nicht nur als Transportverschlüsselung bis zum Providerknoten realisiert) und anbieten muss

- Die Sicherheitsqualität einer E2EE hängt insbesondere auch vom verwendeten Schlüssel ab, u. a. kommt es für die Effektivität der Verschlüsselung maßgeblich darauf an, dass nur die Kommunikationsparteien im Besitz des verwendeten Schlüssels sind.

- Eine wirksame Ende-zu-Ende-Verschlüsselung setzt voraus, dass die Endgeräte der Teilnehmenden sich gegenseitig nachprüfbar authentisieren und für jede Konferenz neue flüchtige Verschlüsselungsschlüssel unter Kontrolle der Konferenzteilnehmer so erzeugt, ausgehandelt bzw. verteilt werden, dass dem Betreiber keine Kenntnisnahme des Schlüsselmaterials möglich ist.

Integration

VKS lassen sich in einige Lernmanagementsysteme integrieren. Hierbei muss darauf geachtet werden, dass die Integration eine in unzulässiger Weise grenzenlose Verkettung personenbezogener Daten ausschließt. Die Gewährleistungsziele der Vertraulichkeit und der Nichtverkettung erfordern auch die Einhaltung der Zweckbindung, die eine Datenverkettung nur in bestimmten Fällen erlaubt.
Prüfen Sie die Lösung des Anbieters, ob die Integrationsschnittstellen steuerbar sind, das heißt, dass die Option der Datenweitergabe transparent erfolgt und nur bewusst und gewollt angestoßen werden kann (Opt-in). Datenweiterleitungen oder Verknüpfungen im Hintergrund sind zu unterlassen.

Homeschooling, Nutzung privater Geräte

Das Lernumfeld der Schüler*innen erstreckt sich räumlich nicht nur auf den Schulcampus, sondern auch auf das Zuhause (Homeschooling). Die eingesetzten privaten Endgeräte (Tablets, Notebooks, PC-Clients) stellen aktuell in der Regel eine durch die Schule nicht gemanagte clientseitige Systemumgebung dar.

- Daher sollte die VK-Software serverseitig die datenschutzfreundlichen Einstellungen steuern und durchsetzen. Dazu bedarf es einer vollständigen Erhebung der angebotenen Funktionen und der Reduzierung auf das notwendige und zulässige Maß. Einstelloptionen, die zu Datenschutzverstößen führen können, sollten nicht dem/der einzelnen Schüler*in überlassen bleiben. (Beispiel: Deaktivierung der Aufzeichnungsoption)
- Die Steuerung sollte regelmäßig durch die Lehrkraft erfolgen.
- Die Lehrkraft muss die Rolle der Konferenzmoderation innehaben und sicherstellen, dass Personen, die unbefugt teilnehmen, erkannt und ausgeschlossen werden.
- Der VK-Dienst muss die Umsetzung eines Rollen- und Rechtekonzepts ermöglichen (siehe Kapitel 4 der Orientierungshilfe der DSK), so dass alle Beteiligten (Lehrkraft und SuS) klare und Rollen basierte Befugnisse und Beschränkungen erhalten.
- Externe Teilnehmer*innen müssen durch einen expliziten Freigabevorbehalt der Lehrkraft kontrolliert werden.

Auswahl von Dienstleistern

- Bei der Auswahl der Dienstleister sollte die Dienstleistung vollständig durch diesen Auftragsverarbeiter ohne Verknüpfung mit internen Diensten der Verantwortlichen erbracht werden.
- Es sollte auch keine von dem Dienst unabhängigen weiteren Auftragsverarbeiter in Anspruch genommen werden. Insbesondere sollte kein Authentifizierungsdienst unbeteiligter Dritter zum Einsatz kommen.

Der Landesbeauftragte für den
Datenschutz Niedersachsen
Adresse Prinzenstraße 5
30159 Hannover
Telefon 0511 120-4500
Fax 0511 120-4599
E-Mail poststelle@lfd.niedersachsen.de
Internet https://lfd.niedersachsen.de