erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

FIfF e. V. – Pressemitteilung

Digitalisierung an Schulen – so nicht!

FIfF kritisiert Digitalpakt mit Windows 10 und Office 365

29. November 2019 – *Der Digitalpakt für Schulen wurde im Mai 2019 für ganz Deutschland – trotz seines Eingriffs in die Föderalisierung – im Rahmen der Strategie für Digitalisierung durch die Bundesregierung verabschiedet. Der Bund stellt hierfür über einen Zeitraum von fünf Jahren insgesamt fünf Milliarden Euro zur Verfügung, davon in dieser Legislaturperiode 3,5 Milliarden Euro.*

Aufgrund des Charakters der Bundesmittel als Finanzhilfen bringen die kommunalen und privaten Schulträger bzw. Länder zusätzlich einen finanziellen Eigenanteil ein. Zusammengenommen stehen dann insgesamt mindestens 5,55 Milliarden Euro bereit. Rein rechnerisch bedeutet dies für jede der ca. 40.000 Schulen in Deutschland im Durchschnitt einen Betrag von 137.000 Euro oder umgerechnet auf die derzeit ca. 11 Millionen Schülerinnen und Schüler eine Summe von 500 Euro pro Schüler in dem Finanzierungszeitraum.

Den Verantwortlichen, somit Schulträgern oder Schulen, steht es zunächst frei, wofür konkret sie diese Gelder zur Modernisierung der IT-Infrastruktur einsetzen. Bereits im laufenden Schuljahr 2019/2020 sollen diese Gelder abgerufen werden, um z. B. Tablets zu kaufen. Zum funktionstüchtigen Einsatz solcher Tablets ist oftmals noch ein schulinternes WLAN zu implementieren. Mit diesen Anschaffungen und dem dauerhaften Betrieb solcher Elemente einer IT-Infrastruktur sind die Mittel pro Schüler verbraucht. Eine Hardware ohne Software ist untauglich. Als Software-Lösung sollen Verträge mit Microsoft geschlossen werden. Den meisten Schulträgern oder Schulen wird eine Lizenz von Office 365 Education unter A1 angeboten, das „Rundum-Wohlfühlpaket", welches mit dem genehmigten Digitalpakt bzw. realisierbaren Kosten für Schulen noch betrieben werden könnte. Umfassendere Lizenzen, wie A3 oder gar A5, mit denen Verantwortliche Software-Dienste konfigurieren könnten, sind jedoch aus Kostengründen wohl kaum vermittelbar.

Das FIfF kritisiert diese Lizenz-Politik und fordert die datenschutzkonforme Verarbeitung der Daten von Schülerinnen und Schülern, die zumeist minderjährig sind. Warum wird hier nicht eine äquivalente Open-Source-Software-Lösung eingesetzt, wie sie z. B. von der Open Business Alliance [1] angeboten wird? Mit solchen Lösungen könnten deutsche Schulen und Institutionen die Kontrolle über ihre Daten behalten, datenschutzkonforme Implementierungen leichter umsetzen und transparent die Datenschutzbestimmungen sicherstellen. Letzteres ist jedoch bei der im Rahmen der oben erwähnten Finanzierung verfügbaren Lösung mit Microsoft 365 unter A1 kaum bis gar nicht zu garantieren. Mindestens sind spezielle Regelungen in der Datenschutzgrundverordnung (DSGVO) anzuwenden, die aufbauend auf Artikel 5, 6 und 7 DSGVO in Artikel 8 DSGVO konkretisiert sind.

Das FIfF fordert Aufklärung, welche Interessen Microsoft verfolgt, denn die Deutsche Telekom AG hat die eigene deutsche Microsoft Cloud zum 31. August 2019 eingestellt. Das Treuhändermodell für Microsoft bei T-Systems ist damit ausgelaufen [2]. Microsoft wird ab 14. Januar 2020 für die Betriebssysteme auf den Servern 2008 und 2008 R2 den Support einstellen und die auf ihnen laufende Software statt dessen in ihre Cloud Azure migrieren, und damit auch alle Daten in Azure in den USA stellen [3]. Danach wird keine Kontrolle von Seiten deutscher Institutionen mehr möglich sein, und es besteht die Gefahr, dass Inhalts- und Verbindungsdaten ohne Wissen oder Genehmigung Betroffener auch an Schulen weiter gesammelt und per Gesetz an die NSA weitergegeben werden können. Solches hat Microsoft in anderen Zusammenhängen bereits getan [4].

Wie gefährlich die – schließlich lebenslang mögliche – Speicherung und Nutzung von Daten, Bildern, Medien- und App-Nutzung und alle Arten von Kommunikation für unsere Kinder ist, ist inzwischen hinlänglich bekannt geworden. Aber die Interessen und fundamentalen Rechte und Freiheiten von Kindern müssen vor allem auch an Schulen garantiert werden: Wenn ein hohes Risiko durch die Anwendung bzw. Umsetzung von Aufgaben im hoheitlichen Bereich durch IT-gestützte Prozesse in einer komplexen IT-Landschaft vorausgesetzt wird (die insbeson-

dere nicht als IT-Landschaft vor Ort beim Schulträger oder in der Schule betrieben wird), ist eine Datenschutz-Folgenabschätzung entsprechend Artikel 35 DSGVO durchzuführen. Mit einer solchen Datenschutz-Folgenabschätzung geht folglich einher, dass für Kinder bzw. Schulen technisch-organisatorische Maßnahmen höheren Anforderungen auch bzgl. der IT-Sicherheit genügen müssen. Vertraulichkeit und Integrität sind ebenso höher zu bewerten (Artikel 25 und Artikel 32 DSGVO). Zur Umsetzung im Besonderen auch dieser datenschutzrechtlichen Anforderungen muss verlangt werden, dass sichere Verschlüsselungen für Transport und Inhalt zu gewährleisten wären.

Das FIfF ruft dazu auf, Einspruch gegen die Regelungen des Digitalpakts einzulegen. Einsprüche gegen die derzeit bestehenden Verträge im Digitalpakt sind sachlich wie zeitlich höchst dringlich, da es Schulen jederzeit möglich ist, sich aus dem Digitalpakt zu bedienen und es bereits einzelne Schulen gibt, die dies getan haben. Was passiert, wenn ein solcher Digitalpakt und damit verbundene Nutzung von Software für Hochschulen geschlossen würde? Ähnliche Implementierungen planen Länder ja in den öffentlichen Verwaltungen, Kommunen und Städten, die ggf. auf Microsoft-Enterprise-Lizenzen basieren sollen.

Referenzen

[1] https://osb-alliance.de

[2] https://www.heise.de/newsticker/meldung/Auslaufmodell-Microsoft-Cloud-Deutschland-4152650.html

[3] https://www.heise.de/ix/meldung/Microsoft-warnt-vor-Support-Ende-des-Server-2008-raet-zum-Cloud-Umzug-4586610.html

[4] https://www.ft.com/content/7d3e0d6a-87a0-11e9-a028-86cea8523dc2

FIfF e. V. – Pressemitteilung

Bündnis fordert Verbot automatisierter Gesichtserkennung

Aktuelle Pläne des Innenministeriums müssen gestoppt werden

9. Januar 2020 – *Ein Bündnis aus zivilgesellschaftlichen Organisationen wendet sich gegen den Vorstoß des Innenministeriums, an 135 Bahnhöfen und 14 Flughäfen automatisierte Gesichtserkennung einsetzen zu wollen. Stattdessen fordert das Bündnis* Gesichtserkennung stoppen *ein Verbot dieser hochproblematischen Technologie in Deutschland. Auch wenn eine Verbesserung der Sicherheit etwa an Bahnhöfen grundsätzlich sinnvoll erscheint, ist automatisierte Gesichtserkennung als Mittel dafür nicht nur ungeeignet, sondern hat immense negative Folgen für Millionen Passanten und Reisende.*

Automatisierte Gesichtserkennung bedeutet eine permanente heimliche Personenüberwachung in öffentlichen Räumen wie Bahnhöfen oder Flughäfen. Die Körperdaten aller Vorbeilaufenden werden dabei erfasst und automatisiert mit Datenbanken abgeglichen, ohne dass die Betroffenen dies bemerken müssen. Damit greift die automatisierte Gesichtserkennung tief in die Rechte und Freiheiten von Menschen ein, wenn biometrische Körperdaten quasi im Vorbeigehen und anlasslos analysiert werden.

„Automatische Gesichtserkennung ist eine Hochrisikotechnologie", erklärt Viktor Schlüter von der Organisation Digitale Freiheit: *„Hohe Falscherkennungsraten, die Diskriminierung von Frauen und People of Color und das enorme Missbrauchspotential stellen eine Gefahr für die Demokratie dar."*

„Dieses unnötige und invasive Biometriesystem ist nur ein weiterer Baustein, den maschinenlesbaren Menschen zu schaffen. Allein durch das zufällige Vorbeilaufen legen wir mit unseren Körperdaten eine digitale Spur, die uns alle auch wegen der Unzuverlässigkeit der eingesetzten Algorithmen in unseren Rechten und Freiheiten einschränkt", sagt Dirk Engling, Sprecher des Chaos Computer Clubs.

„Die optische Vermessung von Gesichtern droht eine weitere Form der anlasslosen Überwachung zu werden, nur diesmal mit detaillierten Körperdaten", fügt Rainer Rehak vom Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung hinzu. *„Wir müssen uns jetzt diesen gefährlichen Plänen in den Weg stellen, bevor immer mehr öffentliche Räume mit biometrischen Erkennungssystemen bestückt werden, die zudem nicht einmal mehr Sicherheit bringen."*

„Der Einsatz dieser Technologie zur Überwachung des öffentlichen Raumes schränkt auch politische Teilhabe ein: Wer fürchten muss, automatisch erfasst zu werden, wird im Zweifel eher nicht an einer Demonstration teilnehmen", gibt Elisabeth Niekrenz von der Digitalen Gesellschaft zu bedenken.

Im Lichte stetig sinkender Kriminalitätsraten in Deutschland besteht nicht nur keinerlei Notwendigkeit für neue, teure und ineffiziente Überwachungsmaßnahmen zur anlasslosen Erfassung von Körperdaten von Reisenden, sondern ist es Zeit, ein Verbot dieser gesellschaftlich schädlichen Technologie in die Wege zu leiten. Ein Verbot automatisierter Gesichtserkennung in Deutschland hat bereits Vorbilder: Mehrere US-amerikanische Großstädte haben den Einsatz der Technologie durch staatliche Stellen im öffentlichen Raum aufgrund der damit verbundenen Gefahren verboten. Der Stadtrat von San Francisco etwa bezeichnete automatisierte Gesichtserkennung als „gefährliche Waffe" sowie als inkompatibel mit einer gesunden Demokratie und verbot ihren Einsatz [0].

Dass die teure Technik überhaupt einsatzreif ist und den erhofften Zweck erfüllt, ist zudem zweifelhaft: In einem Gesichtserkennungstest von Innenministerium und Bundespolizei im Jahr 2018 in Berlin war die Falscherkennungsrate so hoch, dass mehr als jede 200. Person fälschlicherweise erkannt wurde. Dies