
TOP 1 Aktuelle Themen der Berufs- und Gesundheitspolitik

Titel: Cloudbasierte Künstliche Intelligenz (KI) an Behandlungsdaten - nur auf vertrauensvoller Infrastruktur

Beschlussantrag

Von: Fraktion FuturMed29

BESCHLUSSVORSCHLAG:

Die Kammerversammlung der Ärztekammer Nordrhein fordert vom Bundesgesundheitsministerium (BMG), der gematik, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Bundesdatenschutzbeauftragten (BfDI) eine detaillierte Durchführungsbestimmung zur rechtssicheren Anwendung von cloudbasierter Künstlicher Intelligenz (KI), an anonymisierten und nicht-anonymisierten, ärztlichen Behandlungsdaten von Patienten.

Bislang wurde angenommen, es sei durch ausgeklügelte Sicherheitsarchitektur möglich, KI in Cloudspeichern zu betreiben, ohne dass der Cloudbetreiber selbst Zugriff auf den Algorithmus, die dabei verarbeiteten und/oder die generierten Daten bekommen könnte (sogenanntes „Confidential Computing“).

Es hat sich herausgestellt, dass die aktuell üblichen Sicherheitsmaßnahmen, durch eine leicht, im freien Handel, für zehn Euro erhältliche Platine (Raspberry Pi Pico), umgangen werden können. Zwei große Chiphersteller haben öffentlich eingeräumt, an diese Lücke nicht gedacht zu haben. Voraussetzung für den unberechtigten Datenzugriff ist lediglich, mit Administratorenrecht, der Zugang zum Ort, an dem die Cloudserver stehen. Damit haben Cloudbetreiber Zugriff auf Daten, Programme und KI der Nutzer.

Begründung:

Damit gibt es aus Sicht von IT Experten für die Idee des „Confidential Computing“, also des sicheren und vertraulichen KI-Betriebs auf fremder Serverinfrastruktur, keine Grundlage mehr.

Auch wenn die Nachbearbeitung der abgegriffenen Daten als aufwendig gilt, wird dieses Hindernis von den Experten für einen Angreifer, mit den Ressourcen eines Staates, als überwindbar angesehen. In diesem Kontext müssen zukünftig außereuropäische Cloudstandorte als nicht geeignet für den Betrieb von Medizinprodukten angesehen werden. Dies gilt (wegen der US-Gesetzgebung zur Datenherausgabe über Nicht-US-

Angenommen: ☐ Abgelehnt: ☐ Vorstandsüberweisung: ☐ Entfallen: ☐ Zurückgezogen: ☐ Nichtbefassung: ☐

Stimmen Ja: 0

Stimmen Nein: 0

Enthaltungen: 0

Bürger im Ausland) auch für europäische und sogar auch für deutsche Cloudstandorte, die von US-Firmen (mit-)betrieben werden.