



Anfragen zum Plenum zur Plenarsitzung am 30.01.2024 – Auszug aus Drucksache 19/377 –

Frage Nummer 50

mit der dazu eingegangenen Antwort der Staatsregierung

Abgeordneter **Andreas Winhart** (AfD) Ich frage die Staatsregierung, wie viele Hackerangriffe wurden in den letzten drei Jahren auf Unikliniken und andere Gesundheitseinrichtungen in Bayern verzeichnet, wie können Unikliniken und andere Gesundheitseinrichtungen in Bayern ihre IT-Infrastruktur stärken, um sich vor Hackerangriffen besser zu schützen, welche finanziellen Folgen haben Hackerangriffe auf Gesundheitseinrichtungen in Bayern verursacht?

Antwort des Staatsministeriums für Gesundheit, Pflege und Prävention in Abstimmung mit dem Staatsministerium für Wissenschaft und Kunst

An bayerischen Universitätsklinika gab es vereinzelt (erfolglose) Phishing- und Hacker-Attacken in den vergangenen drei Jahren. Eine funktionsfähige, sich auf dem neuesten Stand der Technik befindende IT ist für die Universitätsklinika zum Schutz von Hackerangriffen von erheblicher Bedeutung. Im Rahmen der High Med Agenda stellt der Freistaat daher weitere Mittel zur Verfügung, um den wachsenden Investitionsbedarf abzubauen.

Hinsichtlich der bayerischen Plankrankenhäuser liegen keine über die allgemein zugänglichen Presseinformationen hinausgehende Informationen vor. Die Plankrankenhäuser sind seit 01.01.2022 gesetzlich verpflichtet, Vorkehrungen zu treffen, um die IT-Sicherheit zu gewährleisten (§ 75c Sozialgesetzbuch Fünftes Buch). Dies betrifft nun alle Häuser und ergänzt die Vorschrift des § 8a BSI-Gesetz, der diese Verpflichtung bereits vorher für Häuser der sog. kritischen Infrastruktur vorsah (mehr als 30 000 vollstationäre Fälle im Jahr). Dies entspricht der Tatsache, dass Krankenhäuser nicht Bestandteil der Staatsverwaltung sind, sondern als eigenständige Unternehmen für ihre innerbetrieblichen Angelegenheiten eigenverantwortlich zuständig sind.

Finanzielle Unterstützung bei Maßnahmen zur Verbesserung der IT-Sicherheit bietet der Krankenhauszukunftsfonds (KHZF), der explizit das Thema IT-Sicherheit beinhaltet. So gibt es den eigenständigen Fördertatbestand für die IT-Sicherheit; überdies müssen bei allen anderen Fördertatbeständen aus dem KHZF mindestens 15 Prozent der förderfähigen Kosten für die IT-Sicherheit verwendet werden.

Der Staatsregierung liegen weiterhin keine spezifischen Angaben betreffend die IT-Sicherheit von Arztpraxen oder sonstigen Gesundheitseinrichtungen und auch

keine Informationen zu etwaigen Hackerangriffen sowie durch diese verursachte finanzielle Folgen vor.