



Anfragen zum Plenum zur Plenarsitzung am 13. Mai 2020 – Auszug aus Drucksache 18/7958 –

Frage Nummer 1 mit der dazu eingegangenen Antwort der Staatsregierung

Abgeordneter
**Benjamin
Adjei**
(BÜNDNIS
90/DIE GRÜ-
NEN)

Ich frage die Staatsregierung, welche Einrichtungen und insbesondere systemkritische Unternehmen – wie Produzenten von Medizinprodukten, Pharmaunternehmen, medizinische Forschungseinrichtungen – oder Krankenhäuser in Bayern seit Beginn der Krise Cyberattacken ausgesetzt waren, welche Unterstützung von Staatsseite betroffene Einrichtungen erhalten haben und welche zusätzlichen Gefahren durch die rasche coronabedingte Umstellung auf bislang kaum genutzte IT-Verfahren, mit denen den Anforderungen für Homeoffice, Videokonferenzen und Chats etc. begegnet wird, gesehen werden?

Antwort des Staatsministeriums des Innern, für Sport und Integration

In den wöchentlichen Lagebesprechungen der zu Beginn dieses Jahres neu eingerichteten Informations- und Kooperationsplattform der bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben, der Cyberabwehr Bayern (CAB), wird die aufgrund der Corona-Pandemie besondere Cybersicherheitslage fortlaufend aufmerksam beobachtet und analysiert.

Für den Gesundheitssektor in Bayern lässt sich feststellen, dass die Cyber-Bedrohungslage als kritisch und dynamisch verlaufend eingestuft werden kann. Das Thema „Corona“ wird zwar vermehrt bei Cyber-Angriffen aufgegriffen, allerdings nur unter Verwendung bereits bekannter Modi Operandi. Neue Angriffsvektoren sind im Kontext der Corona-Pandemie bisher nicht aufgetreten. Erkenntnisse zu gezielten Cyber-Angriffen auf systemkritische Unternehmen in Bayern seit Beginn der Krise liegen nicht vor.

Um den durch die COVID-19-Maßnahmen entstehenden erhöhten digitalen Verwundbarkeiten – insbesondere für Unternehmen in dem hier in Rede stehenden Gesundheitssektor – wirkungsvoll entgegen zu treten, wurden durch die CAB sowie das Cyber-Lagezentrum der CAB mögliche cyberrelevante Bedrohungsszenarien identifiziert und bewertet. Ferner wurden organisatorische und operativ-taktische Maßnahmen gemeinsam erörtert, beschlossen und umgesetzt. So hat beispielsweise das Landesamt für Sicherheit in der Informationstechnik (LSI) Empfehlungen für konkrete Maßnahmen zur Erhöhung des Sicherheitsniveaus auf IT-Systemen an

die bayerischen Plankrankenhäuser herausgegeben. In diesem Kontext wurde ferner eine Warnmeldung – aus ganzheitlicher Perspektive der beteiligten Behörden und Einrichtungen der CAB – produziert und an bayerische Krankenhäuser adressiert. Das Cyber-Lagezentrum steht ferner in engem Austausch mit dem Nationalen Cyber-Abwehrzentrum, um frühzeitig potenzielle cyberrelevante Gefahren zu erkennen und sich maßnahmenorientiert abzustimmen.

Die Hinweise auf etablierte Standards bzw. Sicherheitsempfehlungen gelten im Übrigen unabhängig von der Pandemie. Eine Orientierung daran ist stets dringend anzuraten. Dies ist, ebenso wie die Einhaltung der datenschutzrechtlichen Bestimmungen sowie ggf. spezifischer Regulierung im Bereich IT-Sicherheit, durch die Betreiber kritischer Infrastrukturen sicherzustellen. Inwieweit sich durch die Nutzung von Homeoffice, Videokonferenzen usw. eine zusätzliche Gefährdung ergibt, ist nur auf der Grundlage der genauen Kenntnis der vor Ort eingesetzten IT-Infrastruktur konkret zu beurteilen.