UNIVERSITÄTSKLINIKUM
Schleswig-Holstein

Schleswig-Holsteinischer Landtag
Umdruck 20/2979

UKSH, Campus Kiel, Arnold-Heller-Str. 3, Haus V40, 24105 Kiel
UKSH, Campus Lübeck, Ratzeburger Allee 160, 23538 Lübeck

Vorsitzender des Wirtschafts- und Digitalisierungsausschusses
Claus Christian Claussen

Prof. Dr. Dr. h.c. mult. Jens Scholz
Vorstandsvorsitzender/CEO

E-Mail: ceo@uksh.de
www.uksh.de

Campus Kiel
Arnold-Heller-Str. 3, Haus V40, 24105 Kiel
Tel.: 0431 500 - 10001

Campus Lübeck
Maria-Goeppert-Str. 7a, 23538 Lübeck
Tel.: 0451 500 - 10002

Datum: 21.03.2024

Stellungnahme des UKSH zum Bericht der Landesregierung Drucksache 20/1584 (Minister und Chef der Staatskanzlei) über die Cybersicherheit unserer Infrastruktur

Dem UKSH wurde durch Mitteilung vom 28. Februar 2024 vom Wirtschafts- und Digitalisierungsausschuss des Landtages die Möglichkeit gegeben, eine schriftliche Stellungnahme zum ***Bericht über die Cybersicherheit unserer Infrastruktur*** des Landes Schleswig-Holstein zu geben. Diesem kommen wir bezüglich der UKSH-relevanten Themen gerne nach und bedanken uns für diese Möglichkeit.

Wie im Bericht zutreffend ausgeführt sind Krankenhäuser verpflichtet, sich auf interne und externe Schadenslagen vorzubereiten im Rahmen von Krankenhausalarm- und Einsatzplanungen. Dies dient dazu, im Falle von Großschadensereignissen mit einer Vielzahl von Verletzten vorbereitet zu sein und eine Versorgung zu gewährleisten. Dieses findet im UKSH ebenso wie die im Bericht erwähnte Zusammenarbeit mit dem für Katastrophenschutz zuständigen Ministerium statt. Kontaktpersonen für KRITIS und Katastrophenschutz sind vom UKSH dem Ministerium benannt worden.
Bei Sicherheitsvorfällen und sicherheitsrelevanten Ereignissen kommt das UKSH den verschiedenen Meldewegen für die Krankenhäuser gegenüber dem Land nach. Dies betrifft sowohl die Medizintechnik als auch Ereignissen, die im Rahmen von Forschung, Diagnostik und Therapien Strahlung emittieren und für Patienten oder die Bevölkerung relevant sind.
Wie im Bericht erwähnt, sind im Rahmen des Krankenhauszukunftsgesetz (KHZG) geförderte Fördertatbestände mindestens 15 % der gewährten Fördermittel für Maßnahmen zur Verbesserung der Informationssicherheit zu verwenden (§14 Abs. 4 KHZG). Für die derzeit laufenden Projekte innerhalb des Krankenhauszukunftsgesetzes wird diese Quote vom UKSH erreicht werden.
Das Universitätsklinikum Schleswig-Holstein (UKSH) ist auch Teil der kritischen Infrastruktur nicht nur in Schleswig-Holstein, sondern für ganz Deutschland. Daher unterliegt es alle zwei Jahre einer Überprüfung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI), basierend auf dem branchenspezifischen Sicherheitsstandard für die medizinische Versorgung (B3S MV). Diese Prüfungen fanden bereits in den Jahren 2019, 2021 und 2023 statt und zeigten der UKSH-Sicherheitsstruktur Entwicklungspotenziale auf.

Das Universitätsklinikum Schleswig-Holstein (UKSH) sieht sich angesichts der zuletzt stark gestiegenen Cyberbedrohungen erheblichen Herausforderungen gegenüber. Beispiele wie der Hackerangriff auf das Universitätsklinikum Frankfurt, der dort zu einem monatelangen Rückgriff auf traditionelle Kommunikationsmittel führte, verdeutlichen die Notwendigkeit einer robusten

Wissen schafft Gesundheit

Cybersicherheitsstrategie. Ähnliche Vorfälle in anderen Kliniken, die erhebliche finanzielle Schäden nach sich zogen, unterstreichen die breiten Konsequenzen solcher Angriffe, die von Betriebsunterbrechungen über langfristige wirtschaftliche Einbußen bis hin zu Auswirkungen auf die Patientenversorgung reichen.
Um den Herausforderungen zu begegnen, hat das UKSH bereits wichtige Maßnahmen umgesetzt. Dazu gehören der Aufbau eines Informationssicherheitsmanagementsystems (ISMS) und die Optimierung unserer IT-Sicherheitsinfrastruktur, unterstützt durch KRITIS-Fördermittel des Landes Schleswig-Holstein für die Zeiträume 2019-2023 und ursprünglich geplant - jedoch bedauerlicherweise nicht genehmigt - für den Zeitraum 2024-2027. Diese Investitionen haben dazu beigetragen, dass das UKSH heute besser gegen Cyberangriffe gewappnet ist.
Ein aktueller Bestandteil unserer Strategie zur Abwehr von Cyberangriffen ist die Implementierung von Systemen zur Angriffserkennung (SzA), die gemäß dem 2. IT-Sicherheitsgesetz (§ 8a Absatz 1a BSIG) ab dem 1. Mai 2023 verpflichtend sind. Im UKSH sind bereits Elemente von SzA im Einsatz, da diese elementaren Bestandteile einer jeden IT-Sicherheitsinfrastruktur sind. Andererseits sind aufgrund der Bedrohungslagen, Produkte entwickelt worden, die Angriffe auf die Infrastruktur wirksam unterbinden können. Die dazu laufenden Ausschreibungen und geplanten Investitionen von mehreren Millionen Euro über die nächsten drei Jahre sind eine notwendige Voraussetzung, um das Risiko potenzieller Störungen der Versorgungskontinuität nachhaltig zu reduzieren.
In 2022 wurden Gespräche mit Dataport geführt, um die Möglichkeiten eines Security Operation Center (SOC) zu prüfen. Eine weitere Zusammenarbeit hat sich hier nicht sinnvoll ergeben. Das Konzept des SOC wird im UKSH als Bestandteil von SzA mit externen Firmen umgesetzt.

Als Maximalversorger steht das UKSH vor der kontinuierlichen Aufgabe, seine Cybersicherheits-maßnahmen zu stärken und den Stand der Technik für die Informationssicherheit zu halten und sich mit den verschiedenen Aspekten in der differenzierten Aufgabenwahrnehmung zu befassen. Diese Aufgabe ist komplex und beinhaltet neben organisationalen und (IT-)technischen Maßnahmen zur Schärfung des Sicherheitsstatus einen erheblichen – personellen zentralen wie dezentralen – Aufwand zur Schulung, adressatengerechten Kommunikation im präventiven Sinne einerseits und zur Durchsetzung und Prüfung von Vorgaben, Maßnahmen und Schadensabwehr andererseits. Diese Aufgaben sind derzeit nicht ausreichend refinanziert oder budgetär abgebildet.
Dieser zusätzliche, unausweichlich sich entwickelnde Mehraufwand zum Schutz der KRITIS-Funktionalitäten muss durch nachhaltige und auskömmliche Unterstützung des landeseigenen KRITIS-Unternehmens UKSH durch spezifische öffentliche Fördermittel erfolgen, um die Sicherheit unserer Systeme auch in der Zukunft zu gewährleisten und damit die Spitzenversorgung unserer Patientinnen und Patienten auch unter diesen herausfordernden und sich ständig weiterentwickelnden Bedingungen zu gewährleisten.

Mit freundlichen Grüßen

gez. Prof. Dr. Dr. h.c. mult. Jens Scholz
CEO

gez. Peter Pansegrau
CFO