KANTON LUZERN

Regierungsrat

Luzern, 16. Juni 2020

ANTWORT AUF ANFRAGE A 197

Nummer: A 197
Protokoll-Nr.: 722
Eröffnet: 27.01.2020 / Gesundheits- und Sozialdepartement

Anfrage Ursprung Jasmin und Mit. über die Durchführung von Sicherheits-Präventionstests im Luzerner Kantonsspital (LUKS) (A 197)

Vorbemerkungen:
Spitäler und Kliniken sind in vielerlei Hinsicht sensible Einrichtungen und müssen sich und ihre Patientinnen und Patienten in den verschiedensten Bereichen vor Störungen schützen. Wie im Leistungsauftrag des Kantons Luzern festgehalten, führt das Luzerner Kantonsspital (LUKS) ein angemessenes, wirksames Qualitäts- und Risikomanagement. Im LUKS sind verschiedene spezialisierte Fachabteilungen um die physische und technische Sicherheit besorgt. Sie prüfen im Rahmen integrierter Prozesse laufend die bestehenden Risiken und ergreifen die notwendigen Massnahmen. Im Übrigen wird im Spitalbetrieb unterschiedlichsten Sicherheitsaspekten Beachtung geschenkt. Selbstverständlich ist Sicherheit auch ein Führungsthema.

Insbesondere folgende spezialisierten Fachabteilungen des LUKS sind für Sicherheitsbelange und Risikomanagement zuständig:

- Die Fachabteilung Sicherheit und Intervention ist für die Gewährleistung der physischen Sicherheit am LUKS verantwortlich. Schwerpunkte bilden der Objekt- und Personenschutz, der Brandschutz, das Areal- und Verkehrswesen, der Umgang mit Gefahrgut und der Umweltschutz, die Arbeitssicherheit sowie die Unterstützung der Führung bei besonderen Lagen am LUKS.

- Das Informationssicherheitsgremium (ISG) ist für Fragestellungen zu technischen Risiken (inkl. Cyberrisiken) zuständig.

- Die Abteilung Riskmanagement führt jährlich eine Risikobeurteilung durch, welche einen Überblick gibt über die Risikosituation des LUKS. In den Risikogesprächen mit verschiedenen Führungspersonen auf verschiedenen Führungsebenen werden Massnahmen zur Verhinderung und zur Minimierung von Risiken erörtert und die Umsetzung geprüft.

Zu Frage 1: Wie geht das Luzerner Kantonsspital mit Risiken wie Einbruch, Diebstahl (z.B. aus Krankenzimmern, von technischen Geräten oder Medikamenten), Brandstiftung, Sachbeschädigung oder Sabotage (z.B. durch Zugang zu technischen Anlagen) um?

Für den Umgang mit den beschriebenen Risiken sind am LUKS entsprechende Prozesse, Zuständigkeiten und Massnahmen definiert. Beispiele aus verschiedenen Bereichen:

- Zu den präventiven Schutzmassnahmen gehören namentlich die Videoüberwachung der Zugänge sowie besonderer Bereiche. Sicherheitspersonal gewährleistet vor Ort die Sicherheit auf dem Areal. Sowohl auf dem Areal als auch in den Gebäuden finden Kontrollen durch Sicherheits-Patrouillen statt.

- Wenn Gegenstände von Patientinnen oder Patienten abhandenkommen, können diese dem Haftpflicht- und Beschwerdemanagement gemeldet werden. Werden bei der Abklärung und Abwicklung solcher Fälle Schwachstellen und Gefährdungspotentiale erkannt, werden entsprechende Massnahmen eingeleitet. Im Übrigen verfügt das LUKS über eine entsprechende Haftpflichtversicherung.

- Für Sicherheit und Unterstützung im Brandfall sorgt am Standort Luzern die Betriebsfeuerwehr. Die Gebäude sind mit einer Brandmeldeanlage und entsprechenden Löscheinrichtungen ausgerüstet. Dadurch werden Brandereignisse schnell erkannt und können unverzüglich bekämpft werden. Es findet pro Standort eine enge Zusammenarbeit mit den Ortsfeuerwehren statt.

- Im Bereich der Stromversorgung bestehen Redundanzsysteme. So ermöglichen Notstromaggregate im Falle eines Stromausfalls den Weiterbetrieb der wichtigsten Systeme und Anlagen. Die Notstromversorgung wird regelmässig getestet.

- Im Bereich der Informatikinfrastruktur besteht ein Informationssicherheitsprozess inklusive eines Risikomanagementsystems (in Anlehnung an die Standards ISO 27001:2018 / ISO 27002:2018). Innerhalb dieses Systems werden relevante Risiken (z. B. Sabotage technischer Anlagen) durch interne und externe Audits systematisch erhoben und gewichtet. Das ISG empfiehlt technische und organisatorische Massnahmen zur Risikominimierung und prüft deren korrekte Umsetzung.

- Das LUKS verfügt zudem über eine betriebsinterne Notfallorganisation, das sogenannte Dispositiv besondere Lagen (DbL). Eine besondere Lage liegt dann vor, wenn die Aufgaben des Spitals mit ordentlichen Abläufen nicht mehr bewältigt werden können. Dabei kann es sich um interne oder externe Grossereignisse handeln. DbL dokumentiert alle Vorkehrungen und Massnahmen für die Bewältigung von solchen Ereignissen. Um die Abläufe für den Ernstfall zu trainieren, werden regelmässig DbL-Übungen durchgeführt.

Zu Frage 2: Wie werden sensible Bereiche wie zum Beispiel Medikamentenschränke, Laborbereiche, Operationsbereiche, Frühgeburtenstation, Bereiche mit hochwertigen technischen Geräten oder Räume für Elektroverteilung, Sauerstoffversorgung oder Netzwerke abgesichert?

Das LUKS verfügt über ein umfassendes Schliesskonzept, welches die sicherheitsorientierte Zutrittskontrolle zum Gegenstand hat. Es baut unter anderem auf unterschiedlichen Berechtigungsprofilen und definierten Sicherheitszonen auf. Zu besonders sensitiven Bereichen – z.B. mit kritischen technischen Infrastrukturkomponenten wie Elektroverteiler, Netzwerkverteiler, Server usw. – muss der Zutritt dokumentiert sein. Der Zutritt zu diesen Zonen wird nur speziell instruierten und sachverständigen Personen gewährt. Die Berechtigungen verfallen zyklisch und müssen jeweils wieder erneuert werden.

Zu Frage 3: Wie wird seit der Einführung des neuen Informationssystems LUKiS mit den digitalen beziehungsweise mit Cyber-Risiken (z.B. physischer Zugang zum internen Computernetzwerk) umgegangen? Welche neuen Massnahmen wurden dafür beschlossen oder sind geplant?

Das LUKS benötigte schon vor der Einführung des neuen Klinikinformationssystems LUKiS eine funktionierende und sichere IT-Infrastruktur. Entsprechend wurden schon vorher Massnahmen zum Schutz vor Cyber-Risiken umgesetzt. Die organisatorischen und technischen Massnahmen sind vielfältig und ergeben zusammen eine sogenannte IT-Sicherheitsarchitektur, die auf einem Schalenmodell mit verschiedenen Abwehrmassnahmen gegen Angriffe basiert.

Als Betreiber einer kritischen Infrastruktur arbeitet das LUKS bereits heute mit bekannten Bundesstellen zusammen und nutzt deren Services zur Erkennung von Computerviren. Mit der vollständigen Digitalisierung der Spital-Kernprozesse optimiert das LUKS in Zusammenarbeit mit externen Spezialisten diese Erkennungsprozesse weiter und baut ein Kompetenzzentrum für IT-Sicherheit auf. Dieses Zentrum wird den IT-Sicherheitszustand rund um die Uhr überwachen und soll IT-Sicherheitsvorfälle und Angriffe noch rascher erkennen und ein entsprechendes Eingreifen ermöglichen.

Zur Gewährleistung einer höchstmöglichen Informationssicherheit verfügt das LUKS namentlich auch über ein redundantes IT-System. Die Daten des LUKS werden bei professionellen Anbietern in modernsten Datacentern in der Schweiz gespeichert. Diese Datacenter sind sicherheitszertifiziert und werden auch von Dienststellen des Kantons Luzern genutzt, wel-che hochsensible Daten bearbeiten.

Zu Frage 4: Führt das Luzerner Kantonsspital solche Sicherheits-Präventionsmassnahmen, im Fachjargon Penetrationstests (siehe oben beschrieben), betreffend das jetzt gültige Sicherheitsmanagement bereits durch?

Ja, das LUKS führt im Bereich der IT-Sicherheit periodisch Penetrationstests durch. Einerseits werden regelmässig externe Fachfirmen für solche Tests beauftragt, andererseits prüft das LUKS betriebsintern IT-Systeme, die ans Netzwerk angeschlossen werden.

Zu Frage 5: Falls ja, wie sind die Ergebnisse daraus? Wurden allfällige Schwachstellen aufgedeckt? Wie werden die Gefährdungspotentiale eingeschätzt? Welche Massnahmen wurden daraus ergriffen? Falls nein, aus welchen Gründen wird darauf verzichtet?

Über konkrete Testergebnisse, allfällige Schwachstellen und einzelne Massnahmen gibt das LUKS zum Schutz seiner Patientinnen und Patienten und der Funktionsfähigkeit des Spitalbetriebs keine Auskünfte. Generell kann gesagt werden: Die Ergebnisse von Schwachstellenanalysen und Penetrationstests und das Gefährdungspotential entsprechen dem Branchendurchschnitt. Massnahmen zur Steigerung der IT-Sicherheit leiten sich aus den Ergebnissen ab. Dabei werden allfällige Schwachstellen anhand der definierten Risiko-Parameter gewichtet und Massnahmen zur Risikominimierung – in Anlehnung an international anerkannte Standards (z. B. ISO27002) – festgelegt und umgesetzt.

Zu Frage 6: Welche Bereiche unterliegen nicht solchen Sicherheits-Präventionsmassnahmen, im Fachjargon Penetrationstests? Wieso werden in diesen Bereichen diese Tests nicht durchgeführt?

Die Penetrationstests umfassen alle relevanten Bereiche.