Antwort des Staatsrats auf einen parlamentarischen Vorstoss
—
Anfrage Zurich Simon / Rey Alizée 2022-CE-128
Sicherheit der Patientendaten: besserer Schutz für die Freiburgerinnen und Freiburger!

I. Anfrage

Tausende Neuenburgerinnen und Neuenburger haben entsetzt festgestellt, dass ihre medizinischen Daten auf dem Darknet veröffentlicht worden sind. So kann man erfahren, dass der Nachbar HIV-positiv ist, die Bekannte Drogen konsumiert oder eine Angehörige eine Schwangerschaft abgebrochen hat. Auch die Ergebnisse intimster medizinischer Untersuchungen sind auf dem Darknet zu finden. Durch diesen erneuten Datendiebstahl können alle sehen, worüber manche Personen selbst mit ihren engsten Angehörigen nicht sprechen.

Die Arztpraxen, die Opfer dieses Angriffs geworden sind, haben sich wahrscheinlich an die Weisungen ihrer IT-Anbieter gehalten. Solche Hackerangriffe kommen immer häufiger vor; auch die Freiburger Gesundheitsorganisationen und die Patientinnen und Patienten, welche ihre Dienste in Anspruch nehmen, sind vor derartigen Angriffen nicht gefeit. Daher müssen dringend effiziente Unterstützungsmassnahmen geplant werden.

Wir stellen dem Staatsrat deshalb die folgenden Fragen:

1. Was gedenkt der Staatsrat zu unternehmen, um die Datensicherheit der Freiburger Patientinnen und Patienten zu verbessern?
2. Prüft er zusätzliche Anforderungen hinsichtlich Spitalplanung oder mehr Unterstützung bestimmter Akteure, wie beispielsweise die Arztpraxen? Wenn nein, warum hält der Staatsrat ein solches Vorgehen für nicht relevant? Wenn ja, wie möchte er konkret vorgehen?
3. Verfügt das HFR über die notwendigen Mittel, um die ausreichende Sicherheit der bearbeiteten Daten sicherzustellen?
4. Verfügt die Kantonspolizei über die notwendigen Ressourcen zur Durchführung von Ermittlungen?
5. Was empfiehlt der Staatsrat Personen – Patientinnen/Patienten und Gesundheitsorganisationen – die Opfer von Hackerangriffen geworden sind?

1. April 2022

II. Antwort des Staatsrats

Einleitend möchte der Staatsrat daran erinnern, dass die Datensicherheit alle technischen und organisatorischen Massnahmen umfasst, um Daten und Informationen vor Verlust, Manipulation, fremdem Zugriff und Fälschung zu schützen. Dazu gehören die Vertraulichkeit, Integrität und Verfügbarkeit der Daten. Der Datenschutz garantiert seinerseits das Recht jeder Person auf Schutz vor Missbrauch ihrer persönlichen Daten (Art. 13 Abs. 2 Bundesverfassung).

Generell liegt die Durchführung von Massnahmen im Zusammenhang mit der Sicherheit und dem Schutz von Daten in der Verantwortung der Stellen oder Organe, welche die Daten verarbeiten. Auf kantonaler Ebene wird sie durch das Gesetz über den Datenschutz (DSchG) und auf Bundesebene durch das Bundesgesetz über den Datenschutz (DSG) geregelt. Beide Gesetzgebungen sehen für die Verantwortlichen der Bearbeitung (im Prinzip die Eigentümer/innen der Daten) die Verpflichtung vor, deren Sicherheit zu gewährleisten (Art. 8, 12b–12e und 17 DSchG sowie Art. 7 und 10a Abs. 2 DSG). So beinhaltet die Datenschutzgesetzgebung auch Massnahmen zur Datensicherheit. Was speziell die Arztpraxen betrifft, die dem DSG unterliegen, so ist die Ärztin oder der Arzt Verantwortliche/r der Bearbeitung, selbst wenn sie oder er die Informatikleistungen ganz oder teilweise auslagert (Art. 3 Bst. i DSG). Dieser Status bringt eine Reihe von Verpflichtungen in Bezug auf die Datensicherheit mit sich, z. B. die Festlegung von Zugriffsrechten oder die Informationspflicht gegenüber den Patientinnen und Patienten im Falle von Cyberbedrohungen oder -angriffen. Eine der grössten Herausforderungen im Zusammenhang mit dieser Informationspflicht besteht darin, den Patientinnen und Patienten zu ermöglichen, sich vor den direkten Folgen eines unbefugten Eindringens zu schützen und das Risiko weiterer Folgeschäden zu verringern.

Was die Aufsicht betrifft, so sind die eidgenössischen und kantonalen Datenschutzbeauftragten dafür zuständig, die Anwendung der geltenden Gesetze zu überwachen und zusätzlich zur Beratung auch Empfehlungen abzugeben.

So gilt für die Freiburger Gesundheitseinrichtungen (beauftragte Pflegeheime und Spitäler) das kantonale Recht und es ist die kantonale Behörde für Öffentlichkeit, Datenschutz und Mediation (ÖDSMB), die über ihre kantonale Datenschutzbeauftragte und ihre Kommission die Aufgabe hat, die betroffenen Organe zu beraten. Insbesondere bei der Planung der Bearbeitung von Personendaten informiert die ÖDSMB die Personen über ihre Rechte, arbeitet mit den Datenschutzbehörden des Kantons und des Bundes zusammen, führt das Register der Datensammlungen und prüft die Angemessenheit des im Ausland gewährleisteten Schutzes. In Bezug auf die Aufsicht führt die Beauftragte insbesondere systematische Überprüfungen bei den betreffenden Organen durch. Es ist zu beachten, dass es derzeit keine gesetzliche Verpflichtung gibt, wonach eine Datenverarbeitung vor ihrer Implementierung der ÖDSMB vorgelegt werden muss. Nach der Implementierung kann die ÖDSMB jedoch jederzeit eine Kontrolle durchführen. Zu diesem Zeitpunkt wird sie namentlich das Konzept der Informationssicherheit und des Datenschutzes (ISDS), die gesetzlichen Grundlagen und die Verträge, insbesondere die Verträge über die Auftragsbearbeitung, bewerten.

In Anbetracht dessen liegt jede Verarbeitung von Personendaten durch ein öffentliches Organ in der Verantwortung der für das Bearbeiten verantwortlichen Person (d. h. der Leiterin bzw. des Leiters der Stelle). Damit ist sie oder er dafür verantwortlich, die Bestimmungen des DSchG für jene Daten umzusetzen, für die sie oder er zuständig ist.

Für den privaten Sektor, zu dem auch die Arztpraxen gehören, gilt die Bundesgesetzgebung (DSG); der Staat hat keine Aufsichts- oder Eingriffskompetenz. Wie bereits erwähnt ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte die zuständige Behörde für alle Datenschutzfragen in diesem Bereich. Generell berät der Beauftragte private Personen in Fragen des Datenschutzes (Art. 28 DSG).

Wenn eine Person vermutet, dass ihre Personendaten von einer anderen Person widerrechtlich bearbeitet wurden (Verdacht auf Persönlichkeitsverletzung), kann sie nach Artikel 15 DSG eine Strafklage einreichen. Im Idealfall sucht sie vorher das Gespräch mit der oder dem Verantwortlichen der Bearbeitung. Nach demselben Artikel kann die Person vor Gericht insbesondere beantragen, dass das Bearbeiten der Daten, insbesondere die Weitergabe an Dritte, untersagt wird oder dass die Daten berichtigt oder vernichtet werden. Gemäss Artikel 29 DSG klärt der Beauftragte von sich aus oder auf Meldung Dritter hin den Sachverhalt näher ab, wenn Bearbeitungsmethoden die Persönlichkeit einer grösseren Anzahl von Personen verletzen könnten.

Fazit: Bei Cyberangriffen auf Privatpraxen, wie sie im April 2022 im Kanton Neuenburg stattgefunden haben, sind es in der Regel Sicherheitslücken, die von Hackern ausgenutzt werden, um an die Daten zu gelangen. Daher werden meist Schwachstellen auf technischer Ebene (z. B. nicht aktualisierte Software, kein Blockieren von riskanten E-Mail-Anhängen, zu viele Rechte auf den Systemen, nicht genügend strenge Netzwerkfilterung, zu schwache Authentifizierung usw.) als Ursache genannt und nicht die Einhaltung der Datenschutzmassnahmen. Dieser technische Aspekt fällt in den Bereich der Datensicherheit und damit in die Verantwortung der Anbieter und ihrer Nutzerinnen bzw. Nutzer, je nach den vertraglichen Grundlagen, an die sie gebunden sind. In einer Zeit, in der Cyberbedrohungen immer häufiger werden und sich immer rascher weiterentwickeln, ist es die Pflicht der Ärztin oder des Arztes als Verantwortliche/r der Bearbeitung, über die Standards und Empfehlungen zur Informatiksicherheit auf dem Laufenden zu bleiben, um zu verhindern, dass sie oder er ein leichtes Ziel für Hacker wird.

1. *Was gedenkt der Staatsrat zu unternehmen, um die Datensicherheit der Freiburger Patientinnen und Patienten zu verbessern?*

Wie bereits in der Einleitung erwähnt, erinnert der Staatsrat daran, dass der Staat im Privatsektor weder die Kompetenz noch die Verantwortung hat, die Praxis im Bereich der Datensicherheit und des Datenschutzes zu kontrollieren oder zu überwachen, da diese in den Zuständigkeitsbereich des Bundes fallen.

Dennoch hält der Staatsrat infolge der Ereignisse vom 1. April 2022 fest, dass die Direktion für Gesundheit und Soziales (GSD) noch am selben Tag (1. April 2022) eine Information an alle privat praktizierende Ärztinnen und Ärzte im Kanton Freiburg versandt hat. Mit dieser Information sollten sie daran erinnert werden, dass die Sicherheit ihres Primärsystems in der Verantwortung der Anbieter und der Nutzerinnen bzw. Nutzer liegt. In diesem Sinne hat die GSD die Ärztinnen und Ärzte aufgefordert, in Bezug auf Datenschutz und Datensicherheit den Empfehlungen ihres Anbieters zu folgen.

Was den öffentlichen Sektor betrifft, so sind, wie in der Einführung dargelegt, die jeweiligen Stellen für die Datenbearbeitung und die Umsetzung des DSchG verantwortlich. Die Aufsichtsbehörde im Bereich des Datenschutzes handelt hier im Rahmen ihrer Befugnisse, insbesondere durch die Überwachung des Datenschutzes, die Beratung von Institutionen und die Sensibilisierung der Bevölkerung. Im Rahmen der beim Staat Freiburg angebotenen

Weiterbildungen gibt die kantonale Beauftragte beispielsweise einen Kurs zu diesem Thema an der Hochschule für Wirtschaft Freiburg (HSW-FR). Die Behörde referiert auch bei Schulungen, die von der Freiburger Vereinigung zur Organisation überbetrieblicher Kurse (*Association fribourgeoise pour l'organisation des cours interentreprises* – AFOCI) für Praktikantinnen, Praktikanten und Lernende des Staates Freiburg organisiert werden. Darüber hinaus kann sie auf Anfrage bestimmte Einheiten gezielt sensibilisieren und schulen.

Was speziell die vom Kanton beauftragten Spitäler betrifft, so hat die Schweizerische Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren (GDK) jüngst eine zusätzliche Empfehlung im Zusammenhang mit der Informatiksicherheit (s. Antwort auf Frage 2) in ihre Empfehlungen zur Spitalplanung aufgenommen.

Schliesslich sei daran erinnert, dass auch auf Bundesebene verschiedene Massnahmen ergriffen werden: Im Mai 2022 teilte der Bundesrat mit, dass das Nationale Zentrum für Cybersicherheit (NCSC) zu einem vollwertigen Bundesamt werden soll. Das Zentrum wird mit zusätzlichen Ressourcen ausgestattet, vor allem im Bereich des Schutzes vor Cyberrisiken. Des Weiteren hat der Bundesrat im Januar 2022 einen Vorentwurf zur Änderung des Informationssicherheitsgesetzes bezüglich Einführung einer Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen in die Vernehmlassung geschickt. Es ist vorgesehen, dass das NCSC hier die Rolle der Meldestelle übernimmt. Bislang wird die Vorlage von den meisten Kantonen, der Wirtschaft und der Wissenschaft unterstützt.

2. *Prüft er zusätzliche Anforderungen hinsichtlich Spitalplanung oder mehr Unterstützung bestimmter Akteure, wie beispielsweise die Arztpraxen? Wenn nein, warum hält der Staatsrat ein solches Vorgehen für nicht relevant? Wenn ja, wie möchte er konkret vorgehen?*

Laut Bundesgesetz über die Krankenversicherung (KVG, Art. 39) und einschlägiger Verordnung (KVV, Art. 58a und 58b) ist der Staat dazu verpflichtet, ein bedarfsgerechtes Angebot an stationären Spitalleistungen für seine Bevölkerung zu gewährleisten. Vor diesem Hintergrund beurteilt er regelmässig die gesundheitlichen Bedürfnisse der Bevölkerung und erstellt auf Stellungnahme der Kommission für Gesundheitsplanung die kantonale Spitalplanung, auf der die Spitäler aufgeführt sind, die zur Tätigkeit zulasten der obligatorischen Krankenpflegeversicherung (OKP) zugelassen sind. Die Liste wird durch Leistungsaufträge formalisiert, die den einzelnen Einrichtungen nach verschiedenen Kriterien erteilt werden. Der Kanton stützt sich hier vor allem auf die Empfehlungen der GDK.

Das Problem der Sicherheit der Patientendaten und der Schutz der persönlichen Gesundheitsdaten rücken immer mehr in den Mittelpunkt, insbesondere im Zusammenhang mit der Einführung des elektronischen Patientendossiers (EPD). Im Hinblick darauf hat die GDK eine neue Empfehlung zum Schutz personenbezogener Gesundheitsdaten in ihre Empfehlungen zur Spitalplanung aufgenommen.[1]

Der Kanton Freiburg verfolgt die GDK-Empfehlungen zur Spitalplanung aufmerksam und wird darauf achten, dass diese Revisionen im Rahmen der Leistungsaufträge, die bei der nächsten Planung ausgearbeitet werden, umgesetzt werden.

[1] Revidierte GDK-Empfehlungen zur Spitalplanung vom 20. Mai 2022, s. Empfehlung 16.

Für den Bereich der ambulanten medizinischen Versorgung legt das kantonale Gesundheitsgesetz (GesG) fest, dass die Bearbeitung von Gesundheitsdaten der Datenschutzgesetzgebung unterliegt, die – für diesen Bereich – auf Bundesebene angesiedelt ist. Der Staat sorgt jedoch im Rahmen seiner Zuständigkeiten dafür, dass die Kommunikation und das Bewusstsein rund um das Thema Sicherheit für diesen Sektor gewährleistet sind.

3. *Verfügt das HFR über die notwendigen Mittel, um die ausreichende Sicherheit der bearbeiteten Daten sicherzustellen?*

Wie bereits erwähnt liegt jede Verarbeitung von Personendaten durch ein öffentliches Organ in der Verantwortung der für das Bearbeiten verantwortlichen Person (d. h. der Leiterin bzw. des Leiters der Stelle).

Die Mittel zur Gewährleistung der Datensicherheit für das freiburger spital (HFR) wie auch für das Freiburger Netzwerk für psychische Gesundheit (FNPG) wurden bis 2022 durch die Verordnung über das Informatik- und Telekommunikationsmanagement in der Kantonsverwaltung auf kantonaler Ebene geregelt.

Diese Verordnung wurde im Juli 2021 durch die Verordnung über die Governance der Digitalisierung und der Informationssysteme des Staates (Art. 2 Abs. 2) abgelöst, die präzisiert, dass gewisse öffentliche Einrichtungen Freiburgs, darunter das HFR und FNPG, organisatorisch autonome Einheiten sind. Sie können ihre Informatikstrategie selber festlegen und ihre Informationssysteme eigenständig verwalten. Laut derselben Verordnung können die autonomen Einheiten oder Dritte mit dem Amt für Informatik und Telekommunikation (ITA) Vereinbarungen abschliessen, um seine Leistungen in Anspruch zu nehmen. Das Übergangsrecht sieht vor, dass die aktuell für die autonomen Einheiten erbrachten Informatikdienstleistungen innerhalb von zwei Jahren in Vereinbarungen formalisiert werden müssen. So erfolgte die Kündigung der Rahmenvereinbarung zwischen dem HFR und dem ITA am 31. Dezember 2020 mit Wirkung zum 31. Dezember 2022. Eine Verlängerung dieser Vereinbarung, um die Migration unter den besten Bedingungen zu ermöglichen, wird derzeit diskutiert. Nichtsdestotrotz wird das HFR nach Ablauf dieser Verlängerung seine Verpflichtungen in Bezug auf Datensicherheit und Datenschutz allein wahrnehmen, sofern zwischen dem ITA und dem HFR keine anderslautende Vereinbarung im Bereich der Informatik getroffen wird.

Aktuell und mindestens bis zum Ablauf der Frist für die Umsetzung der Verordnung über die Governance der Digitalisierung und der Informationssysteme des Staates (1. Juli 2023) werden die IT-Infrastrukturen des HFR und des FNPG (Netzwerk, Server und Backups) vom ITA verwaltet, das für die Sicherheit dieser Informatikmittel verantwortlich ist. Wie einleitend erwähnt, sind es im Falle eines Cyberangriffs meist diese Mittel, die ins Visier genommen werden.

In Bezug auf den Datenschutz sind das HFR und das FNPG dafür verantwortlich, einen sicheren Zugriff und eine sichere Nutzung der verschiedenen IT-Systeme zu gewährleisten. Auf die medizinischen Daten von Patientinnen und Patienten können nur berechtigte Mitarbeitende zugreifen, entsprechend ihrem Profil (Verwaltung und Kontrolle der Zugriffsrechte). Diese Zugriffe sind personenbezogen, entsprechen den aktuellen, vom ITA herausgegebenen Sicherheitsstandards und sind vollständig rückverfolgbar. Der Zugriff durch externe Partner (IT-Anbieter) ist streng geregelt und nur über Konten und Plattformen möglich, die vom ITA bereitgestellt werden.

An dieser Stelle sollte schliesslich daran erinnert werden, dass das NCSC über die Austauschplattform der Melde- und Analysestelle Informationssicherung (MELANI) den Informations- und Wissensaustausch im Gesundheitssektor fördert. Darüber hinaus stellt das NCSC Instrumente zur Sicherheitsbewertung für Spitäler bereit (s. Antwort auf Frage 5).

4. *Verfügt die Kantonspolizei über die notwendigen Ressourcen zur Durchführung von Ermittlungen?*

Bei der Freiburger Kantonspolizei gibt es Inspektorinnen und Inspektoren, die auf Cyber-Kriminalität spezialisiert sind, sowie Spezialistinnen und Spezialisten für digitale Ermittlungen.

Die Ressourcen, die heute für Cyber-Ermittlungen bereitgestellt werden, ermöglichen eine angemessene Reaktion auf diese neuen Kriminalitätsphänomene. In der Tat besteht aber noch viel Verbesserungspotenzial bei der Auswertung und Identifizierung digitaler Spuren für die Ermittlungen.

2021 wurde diese Herausforderung im Rahmen des Antrags auf Aufstockung der Mitarbeitendenzahl der Kantonspolizei identifiziert. Mit dem Dekret über den Bestand der Kantonspolizei wurde eine zweckdienliche Antwort vorgeschlagen, die der Grosse Rat am 5. November 2021 verabschiedete. Die Kantonspolizei wird so noch dieses Jahr in der Lage sein, ihr Dispositiv umzusetzen und ein Kommissariat schaffen, das sich auf die Bekämpfung der Cyberkriminalität spezialisiert, mit einer deutlichen Erhöhung der Zahl der Spezialistinnen und Spezialisten mit spezifischen Kenntnissen und Kompetenzen im Bereich der Digitalisierung.

Der Kanton wird so über eine verstärkte Struktur für die Bereiche Cyber-Straftaten, Datensicherung und digitale Spurenauswertung sowie für die Ausbildung verfügen. Dies nicht nur was die Mitarbeitenden der Kantonspolizei betrifft, sondern auch bei ihren Partnerinnen und Partnern.

Die richtige Rekrutierung und Bindung dieser Spezialistinnen und Spezialisten sind eine grosse Herausforderung für die Polizei, sind doch diese Kompetenzen weit über den Kanton hinaus gefragt.

Der Zeitplan für die Verstärkung dieses neuen Cyber-Kommissariats hängt aber von den logistischen Eventualitäten ab, wie der Suche und der Einrichtung von physischen Arbeitsplätzen. Die Auslastung der Arbeitsplätze im BAPOL (Gebäude der Kriminalpolizei an der Place Notre-Dame in Freiburg) hat heute ihre Grenzen erreicht. Der Bau des neuen Gebäudes der Gerichtspolizei in Granges-Paccot wird noch mehrere Jahre dauern. Diese logistische Einschränkung ist eine Hürde für den Ausbau der Kriminalpolizei und insbesondere für das zukünftige Kommissariat für Cyberkriminalität. Die Verlegung einer Brigade der Kriminalpolizei in ein anderes Gebäude des Staats Freiburg würde ermöglichen, diese Einschränkung zu überbrücken.

5. *Was empfiehlt der Staatsrat Personen – Patientinnen/Patienten und Gesundheitsorganisationen – die Opfer von Hackerangriffen geworden sind?*

Die beste Empfehlung bleibt die Prävention und der Schutz der Unternehmen. Um die Risiken in Zusammenhang mit Schadsoftware zu senken, gelten namentlich folgende Empfehlungen:

> Erstellen Sie regelmässig eine Sicherungskopie (Backup) Ihrer Daten auf einem externen Medium, das Sie nach dem Backup-Vorgang vom Computer trennen;

> Halten Sie Betriebssystem, Software und Antivirenprogramme auf dem neuesten Stand. Wenn möglich sind automatische Aktualisierungen zu bevorzugen;
> Schützen Sie alle Ressourcen, die über das Internet zugänglich sind (z. B. Terminalserver, RAS, VPN-Zugriffe usw.) mit einer Zwei-Faktor-Authentifizierung;
> Blockieren Sie im Postfach E-Mails, die gefährliche Dateien enthalten, z. B. Office-Dateien mit Makros;
> Verwenden Sie starke Passwörter (mindestens 10 Zeichen, darunter Zahlen, Grossschreibung, Kleinschreibung und Sonderzeichen);
> Prüfen Sie die Geräte regelmässig mit einem vollständigen Systemscan auf Infektionen;
> Schulen Sie die Mitarbeitenden regelmässig und führen Sie Übungen durch.

Für Opfer eines Angriffs gelten folgende Empfehlungen:

> Die infizierten Rechner vom Firmennetzwerk und vom Internet trennen, wenn ein Angriff stattfindet. Sofort den Informatikdienst oder den Anbieter kontaktieren, damit er die notwendigen Massnahmen ergreift;
> Wenn das System bereits blockiert ist, das möglicherweise geforderte Lösegeld nicht zahlen, nichts anfassen und sofort mit der Polizei Kontakt aufnehmen. Wenn möglich die verschlüsselten Daten mit Sicherungskopien, die mithilfe des Informatikdienstes und/oder spezialisierten Anbietern hergestellt wurden, wiederherstellen;
> Strafanzeige erstatten;
> Versuchen, die Sicherheitslücke, die den unerlaubten Zugriff ermöglichte, zu identifizieren und Massnahmen zu ergreifen, damit dies nicht wieder geschieht.

Neben diesen Empfehlungen laufen verschiedene Aktionen auf nationaler Ebene, um die verschiedenen Akteurinnen und Akteure des Gesundheitsbereichs über die Datensicherheit und den Datenschutz zu informieren.

Das Netzwerk digitale Ermittlungsunterstützung Internetkriminalität (NEDIK) beispielsweise hat in Zusammenarbeit mit dem NCSC und Swiss Cyber Experts eine Checkliste mit Empfehlungen an die Sicherheitsverantwortlichen der Informationssysteme einer Organisation veröffentlicht.[2] Ausserdem ermöglichte eine vom Bund und dem NCSC unterstützte Initiative die Schaffung eines einfachen und schnellen Onlinetests, der zwar kein Sicherheitsaudit ersetzt, aber allen Unternehmen ermöglicht, ihre Schwächen und ihr Verbesserungspotenzial zu erkennen (www.cybersecurity-check.ch).

Auch andere nationale Organisationen bieten den verschiedenen Akteurinnen und Akteuren des Gesundheitsbereichs Unterstützung bei der Informatiksicherheit. So erarbeiteten Fachpersonen der Spitalinformatiksicherheit in Zusammenarbeit mit H+ einen Katalog mit den einzuhaltenden Mindestanforderungen für die Akquisition und den Betrieb von Fremdsystemen im Spitalbereich, zu denen die medizinischen Geräte gehören.[3] Auf ähnliche Weise unterstützt die FMH ihre Mitglieder beim digitalen Wandel und veröffentlichte ebenfalls eine Reihe von Minimal-anforderungen an den IT-Grundschutz für Praxisärztinnen und Praxisärzte.[4] Letztlich veröffentlichte Curaviva verschiedene Dokumente, mit denen insbesondere Einrichtungen eine

[2] Cyberattacke – was tun? Checkliste für CISOs für den Fall eines Cyberangriffs (admin.ch).
[3] Cyber Security (hplus.ch).
[4] IT-Grundschutz | FMH.

Standortbestimmung der Sicherheit und des Schutzes ihrer Daten vornehmen und ihre Dispositive in diesem Bereich konsolidieren oder verbessern können.[5]

Abschliessend ist zu erwähnen, dass infolge des Cyberangriffs vom 1. April 2022 spezifisch für Arztpraxen im Rahmen einer von der Medizinischen Gesellschaft der Romandie (SMSR) am 11. Mai organisierten Konferenz zur Cybersicherheit der Arztpraxen verschiedene Denkansätze zur Datensicherheit besprochen wurden. Zu diesen Ansätzen gehören namentlich die Verbesserung der Information und Kommunikation zwischen Praxen und Informatikanbietern, eine allfällige Revision der bewährten Vorgehensweisen im Bereich der Computersicherheit sowie die Stärkung der diesbezüglichen Schulung während und nach der Ausbildung.

20. September 2022

[5] CURAVIVA.