Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren
Conférence des directrices et directeurs cantonaux de la santé
Conferenza delle direttrici e dei direttori cantonali della sanità

Faktenblatt

Studie der Global Digital Health Partnership Cyber Security

Ausgangslage

2018 wurde die Gobal Digital Health Partnership (GDHP) gegründet. Es handelt sich dabei um eine Zusammenarbeit zwischen verschiedenen Ländern und deren Behörden sowie der Weltgesundheitsorganisation (WHO). Die Schweiz beteiligt sich an dieser Partnerschaft. Deren Ziel ist, einen Austausch über bewährte Strategien und Verfahren für digitale Gesundheitsdienste aufzubauen und so Erkenntnisse zur Bereitstellung besserer digitaler Gesundheitsdienste für die Teilnehmerländer zu generieren. Im Rahmen dieser Zusammenarbeit wurden Berichte zu unterschiedlichen Schlüsselthemen erstellt, wie z.B. «Interoperabilität», «Cybersicherheit», «Evidenz und Evaluation» und «Zugang der Bürgerinnen und Bürger zu ihren Gesundheitsdaten».

Im Februar 2019 nahm der GDHP-Workstream Cybersicherheit am Gipfel in Neu-Delhi die Arbeit am Whitepaper *Securing digital health: initial reflections for steering global cyber security efforts in health (Sicherung der digitalen Gesundheit: erste Überlegungen zur Steuerung der globalen Cybersicherheitsbemühungen im Gesundheitswesen)* auf. Seit der Lancierung dieses Dokuments arbeiten die am genannten Workstream Beteiligten gemeinsam an der Entwicklung eines *Foundational Capabilities Framework* (FCF, Rahmen für Grundkompetenzen).

Das vorliegende Faktenblatt fasst die wichtigsten Ergebnisse des Berichts zur Cybersicherheit von 2020[1] zusammen. Die Kommentare, Fakten und Argumente stammen von der GDHP.

Ziel der Forschungsarbeit

Da die digitale Revolution im Gesundheitswesen immer schneller voranschreitet, muss sichergestellt werden, dass dem Nutzen und Potenzial dieses Wandels durch die Bereitstellung robuster Cybersicherheitssysteme in allen Teilnehmerländern Rechnung getragen wird. Da sich die Teilnehmerländer in verschiedenen Stadien und mit unterschiedlichem Stand auf ihrem Weg befinden und dabei Interoperabilität anstreben und in den Mittelpunkt stellen, besteht die Möglichkeit und Notwendigkeit, ein einheitliches Rahmenwerk für Cyberkompetenzen im Gesundheitswesen zu schaffen. Dieses sollte nicht nur die klassischen Aspekte der Cybersicherheit abdecken, sondern spezifisch auch die Risiken einbeziehen, die von älteren medizinischen Geräten, die ins Netz eingebunden werden, sowie von der Entstehung der medizinischen IoT-Landschaft (Internet of Things oder Internet der Dinge) ausgehen.

[1] Global Digital Health, *2020 Global Digital Health Partnership Launches White Papers*, https://www.gdhp.org/gdhp-whitepapers, Zugriff am 21. August 2020.

Das Hauptziel dieser Forschungsarbeit ist, gemeinsame Chancen und Herausforderungen zu erkennen und zu verstehen. Die Arbeit liefert den Teilnehmerländern auch den eigentlichen Kompetenzrahmen (Foundational Capabilities Framework, FCF) als zusätzliches Instrument, mit dessen Hilfe sie ihre eigenen jeweiligen Cybersicherheitsprogramme, Kompetenzen und Strukturen in konsistenter und vorhersehbarer Weise strukturieren, gestalten und messen können.

Dieses Forschungspapier umfasst sieben Kernbereiche. Der Fragebogen beinhaltet 59 Fragen aus diesen Kategorien. Fast die Hälfte der an der GDHP Beteiligten lieferte Beiträge zu diesem Forschungspapier, was die Repräsentativität der Arbeit gewährleistet und zur Zuverlässigkeit und Validität der Ergebnisse beiträgt.

Wichtigste Ergebnisse

Die Ergebnisse gaben einen Einblick in die bestehenden Grundkompetenzen wie auch in den Schwerpunkt der Verbesserungen in den Teilnehmerländern in den nächsten 18 Monaten.

Aktueller Stand: Die schwächsten Kompetenzkategorien sind «Cyber-Resilienz, Geschäftskontinuität und Notfallwiederherstellung» sowie «Resilienz und Sicherheit der Lieferkette». Die GDHP anerkennt die Notwendigkeit, Länder mit schwierigerem Stand durch die Förderung des internationalen Austauschs zu unterstützen. Die stärkste Kategorie ist «Verständnis der strategischen Bedrohung», wobei viele Teilnehmerländer vorhandene nationale Kompetenzen und Erfahrungen nutzen, um den Fortschritt im Gesundheitssektor zu beschleunigen. Die GDHP bietet eine Plattform für den Austausch von Informationen zu Bedrohungen, die bereits gute Fortschritte ermöglicht hat und die Möglichkeit bietet, den internationalen Austausch zu unterstützen.

Geplanter Stand in 18 Monaten: Einerseits legen die Teilnehmerländer den Schwerpunkt nicht auf «Cyber-Resilienz, Geschäftskontinuität und Notfallwiederherstellung». Dennoch ist dieser Aspekt entscheidend für die Verfügbarkeit von Dienstleistungen im Gesundheitswesen. Andererseits gehen alle Beteiligten von einer deutlichen Verbesserung der «Resilienz und Sicherheit der Lieferkette» aus.

1. Ausrichtung der klinischen Ergebnisse

Sicherheitsmanagementprozesse helfen bei der Identifizierung kritischer klinischer Anlagen und Systeme. Ihr Einsatz ermöglicht eine risikogesteuerte Priorisierung der Anlagen- und Netzwerkhärtung, die Anwendung von Sicherheitskontrollen und eine Risikominderung. Die wichtigsten Herausforderungen stehen im Zusammenhang mit Sicherheitsbedrohungen im Gesundheitswesen. Dies ist darauf zurückzuführen, dass es technisch wie auch strategisch schwierig ist, Informationen zu Bedrohungen und verwertbare Erkenntnisse rechtzeitig zu verbreiten. Weitere Herausforderungen liegen in der Aufklärung und Sensibilisierung der gesamten Führungsspitze, damit diese versteht, dass das Cybersicherheitsrisiko ein echtes strategisches Geschäftsrisiko ist, das ohne entsprechende Massnahmen zu katastrophalen Ergebnissen und der Unfähigkeit, die Patientenversorgung und die gewünschten Patientenresultate zu gewährleisten, führen kann.

2. Cyber-Reaktionsbereitschaft und -Wiederherstellung

Definierte Eskalationspfade und -pläne für Vorfälle sind in allen Teilnehmerländern üblich. Eine Reihe von Reaktionsplänen und -prozessen sind jedoch nach dem Vorbild bestehender Abläufe zur Reaktion auf IT-Vorfälle statt cybersicherheitsspezifisch aufgebaut. Tests werden zudem eher nach grösseren Vorfällen anstatt regelmässig durchgeführt.

3. Verständnis der strategischen Bedrohung

Spezielle Teams zur Ermittlung von Bedrohungen im Gesundheitssektor sind in allen Teilnehmerländern üblich, wodurch gezieltere und spezifischere Erkenntnisse gewonnen und an bestimmte Empfänger weitergegeben werden können. Zwar verfügt eine Mehrheit der Teilnehmerländer über solide Informationen zu Bedrohungen, doch nicht alle haben eine strategische und präzise Sichtweise. Die Unterstützung durch Behörden, Strafverfolgungsstellen sowie branchenübergreifende Beratungsgruppen ist in allen Teilnehmerländern üblich, aber die Art und Tiefe der Zusammenarbeit variiert je nach Land.

4. Cyber-Resilienz, Geschäftskontinuität und Notfallwiederherstellung

Eine verstärkte Regulierung (z.B. durch europäische Richtlinien) verbessert die Kompetenz nicht direkt und hat in einigen Fällen die unbeabsichtigte Folge, dass eher eine Kultur des Abhakens von Checklisten vorangetrieben wird als ein kultureller Wandel, der erforderlich ist, um einem strategischen Geschäftsrisiko zu begegnen. Eine Reihe der Teilnehmerländer geht mit spezifischen Fragen an Cyber-Resilienz, Geschäftskontinuität und Notfallwiederherstellung sowie an die Kompetenzen und Verpflichtungen zu sicherem Design heran.

5. Verhältnismässigkeit und Wirksamkeit von Budget und Investition

Die Teilnehmerländer verfügen in der Regel über ein spezielles Budget für Cybersicherheit im Gesundheitswesen, das sich jedoch nicht immer von IT-Budgets unterscheidet, was zu übermässig technologieorientierten Investitionsprofilen führt, bei denen Schlüsselpersonen und wichtige Prozesselemente ausser Acht gelassen werden. In manchen Ländern werden das Cybersicherheitsbudget und die entsprechenden Investitionen ausserhalb des Gesundheitswesens durch eine Dritt-Regierungsstelle kontrolliert. Dies ermöglicht zwar bis zu einem gewissen Grad eine stärkere Bündelung der finanziellen Ressourcen, verringert jedoch die Flexibilität und Kontrolle der Gesundheitsbehörden.

6. Governance, Kultur und Führung

Es gibt eine gewisse Überschneidung der Zuständigkeiten zwischen dem Gesundheitssektor und anderen Regierungsstellen oder den Strafverfolgungsbehörden, was zu Verwirrung oder mangelnder Klarheit in Bezug auf die Entscheidungsfindung und die Übernahme von Risiken führt. Allgemein thematisiert werden die Möglichkeiten zur Weiterentwicklung des systemweiten, nationalen Betriebsmodells für Cybersicherheit innerhalb des Gesundheitswesens. Dabei ist sicherzustellen, dass das Modell die umfassenderen nationalen Strukturen und Kompetenzen im Bereich der Cybersicherheit ergänzt und sich gegebenenfalls in sie einbinden lässt. Es hat sich ein neuer Trend zur Ernennung leitender Sicherheitsbeauftragter herausgebildet, aber dies muss durch Schulungen auf Geschäftsleitungsebene und systemweite Sensibilisierungsmassnahmen weiter unterstützt werden.

7. Resilienz und Sicherheit der Lieferkette

Vorschriften wie die Datenschutz-Grundverordnung der EU bewirken, dass die Verpflichtungen zur Cybersicherheit in der Lieferkette zunehmen. Es mangelt jedoch an standardisierten Formulierungen und Entwürfen von Klauseln und vertraglichen Verpflichtungen, was zur Folge hat, dass Inkonsistenzen eingeführt werden und in einigen Fällen der Lieferant von Verbindlichkeiten und Verpflichtungen entbunden wird.

Vertragsklauseln und Verpflichtungen sowie die Umsetzung von Schutzvorkehrungen werden in erster Linie durch den Datenschutz und weniger durch Bedenken und Verpflichtungen im Bereich der Cybersicherheit vorangetrieben.

Geplanter Stand in 18 Monaten

Cybersicherheit bleibt ein sensibles Thema. Planung, Erwartungen und Erkenntnisse für die nächsten 18 Monate werden von den Mitgliedsstaaten nicht ohne Weiteres ausgetauscht. Sie alle gehen jedoch davon aus, dass sie ihre Kompetenzen in Bezug auf klinische Ergebnisse, Risikobewertungen und insbesondere ihre Governance verbessern werden. Die wichtigsten Verbesserungen konzentrieren sich auf die Einführung neuer Rollen und Befehlshierarchien für die Cybersicherheit.

Finanzen, Cyber-Resilienz und Notfallwiederherstellung sind die Schwachstellen der zukünftigen Entwicklungen. Für die jüngsten Trends ist das Grundprinzip nicht sofort klar, aber eine Arbeitshypothese ist, dass Geschäftskontinuität und Notfallwiederherstellung weiterhin in herkömmliche IT-Prozesse eingebettet sind und von diesen vorangetrieben werden.

Schliesslich stellen ältere Verträge und Produkte nach wie vor eine Herausforderung dar, aber die Beteiligten konzentrieren sich darauf sicherzustellen, dass neue Verträge und Vertragserneuerungen die korrekten Verpflichtungen an die Lieferkette weitergeben und bei Missachtung entsprechende Sanktionen vorsehen.