6 Schlussfolgerung und Ausblick

In diesem Kapitel wird die Schlussfolgerung beleuchtet sowie Handlungsempfehlungen genannt. Diese Tabelle gibt einen Überblick der kategorisierten identifizierten Themen.

Kategorie	Dringlichkeit	Handlungsempfehlungen	Instrument	Verantwortung	Betroffene Branche				
					Med. Stat.	Med. Ambul.	Arznei-mittel	Labo-re	Med.-techn.
Umgang mit akuten technischen Problemen	Akut	• Absicherung von unkontrollierten Fernwartungszugängen	Technische Maßnahme	Betreiber	X	X	X	X	X
		• Adressierung von potenziellen Schwachstellen in IT-basierten insb. vernetzten Medizinprodukten	Technische Maßnahme	Betreiber, Hersteller					X
		• Ausbau von Netzwerkzugangskontrollen & Mobile Device Management	Technische Maßnahme	Betreiber	X	(X)	X	X	
		• Trennung von medizinischen und nicht-medizinischen Netzwerken	Technische Maßnahme	Betreiber	X	X	X	X	X
	Mittelfristig	• Verschärfung der Anforderungen an Zutritts- und Zugriffskontrollen	Technische Maßnahme	Betreiber		X			
Änderungen der Randbedingungen	Kurzfristig	• Ergänzung der Zulassungsverfahren für IT-basierte insb. vernetzte Medizinprodukte	Regulatorische Maßnahme	Bundesregierung					X
		• Zügige Ausarbeitung der KRITIS-Verordnung inkl. spezifischer Kriterien für den Sektor Gesundheit unter Einbeziehung der Verbände und Betreiber	Regulatorische Maßnahme	BMI	X	X	X	X	
	Mittelfristig	• Proaktive Überprüfung der Kriterien in der KRITIS-Verordnung nach 2 bis 3 Jahren	Regulatorische Maßnahme	BMI	X	X	X	X	
		• Erarbeitung eines Finanzierungskonzepts zur Steigerung der IT-Sicherheit	Finanzpol. Maßnahme	BMG	X	X	(X)	X	(X)
		• Prüfung des Regelungsbedarfs auch für nichtkritische Betreiber	Regulatorische Maßnahme	Bundesregierung	X	X	X	X	X
	Langfristig	• Harmonisierung der Gesetzgebung im Schnittpunkt IKT und Gesundheitswesen	Regulatorische Maßnahme	Bundesregierung	X	X	X	X	X

Kategorie	Dringlichkeit	Handlungsempfehlungen	Instrument	Verantwortung	Betroffene Branche				
					Med. Stat.	Med. Ambul.	Arznei-mittel	Labo-re	Med.-techn.
Notwendige Schritte zur Umsetzung der Vorgaben aus dem IT-Sicherheitsgesetz	Kurzfristig	• Aktivere Mitgestaltung der Umsetzung des IT-Sicherheitsgesetzes durch die Branchen	Engagement Branchenvertreter	Betreiber, Verbände	X	X	X	X	X
		• Gründung eigener Branchenarbeitskreise bzw. Teilnahme an existierenden	Engagement Branchenvertreter	Betreiber, Verbände		(X)	X	X	X
		• Intensivierung der Arbeit im existierenden Branchenarbeitskreis, insb. zur Entwicklung und Umsetzung von Branchenstandards	Engagement Branchenvertreter	Betreiber, Verbände	X	(X)			
		• Intensivierung der Kommunikation zur Schaffung von Transparenz über weiteres Vorgehen und Auswahlkriterien der kritischen Betreiber bzgl. KRITIS-Verordnung	Kommunikative Maßnahme	BMI, BSI	X	X	X	X	X
Weiterer Forschungsbedarf	Mittelfristig	• Überprüfung des aktuellen Branchenschnittes im KRITIS-Sektor Gesundheit	Methodische Anpassung	BMI, BSI	X				
		• Neubewertung der IT-Sicherheit der ambulanten Versorgung nach Roll-out der TI und Prüfung der IT-Sicherheit der vorhandenen Bestandnetze in den Branchen	Weitergehende Analyse	BAK, Betreiber, Verbände		X			
		• Feinanpassung der MIKI-Methodik auf Besonderheiten des Gesundheitswesens	Methodische Anpassung	BMI, BSI	X	X	X	X	X
		• Vertiefende Analyse des Bereichs Medizintechnik	Weitergehende Analyse	Betreiber, Verbände					X
	Langfristig	• Gewährleistung der sektor- und branchenübergreifenden Abstimmung, bspw. durch Aufbau eines kontinuierlichen Dialogformats	Weitergehende Analyse	Betreiber, Verbände, Bundesregierung	X	X	X	X	X
		• Fortwährende Aktualisierung ausgewählter Studieninhalte durch das BSI sowie externe Validierung der Ergebnisse in 3-5 Jahren aufgrund der zunehmenden Digitalisierung	Weitergehende Analyse	BSI	X	X	X	X	X

6.1 Umgang mit akuten technischen Problemen

Absicherung von unkontrollierten Fernwartungszugänge:

Unbefugte können in das System eindringen und könne sich überall Zugang beschaffen. Das führt zur Beschränkung von Versorgungsdienstleistungen, außerdem den Verlust von sensiblen Daten. Deswegen will man die Fernwartungszugänge absichern oder komplett deaktivieren, wenn es nicht möglich ist.

Potentielle Schwachstellen in IT-basierten Medizinprodukten:

Eine Schwachstelle ist, dass die Betriebssysteme von Medizingeräten oft veraltet sind. Außerdem wird manchmal das Standartpasswort nicht geändert und das führt zu leichter angreifen kann.

Wenn ein Betreiber versucht ein Patch durchzuführen, wird er selbst zum Hersteller und dann braucht man eine erneute Zulassung.

Netzwerkzugangskontrollen und Mobile Device Management:

Sind oft unzureichend, um die Sicherheit zu gewährleisten. Die Aubau der Netzwerkkontrollen sind besonders bei der medizinischen stationären Versorgung, der Versorgung mit Arzneimitteln und Impfstoffen sowie der Laboranalytik wichtig. Das alles trifft auch auf die Ambulante Versorgung zu, alle müssen sicherstellen, dass die genutzten Netzwerke sicher sind.

Medizinische und nicht-medizinische Netzwerke:

Diese Netzwerke sollte man voneinander sperren, dadurch kann man Sicherheitslücken umgehen, da unverschlüsselte E-Mails oder der Aufruf schädlicher Websites begrenz werden.

Verschärfung der Anforderungen an Zutritt- und Zugriffskontrollen

Das kann nur mittelfristig umgesetzt werden, da Leistungserbring es kritisch betrachten. Es wird gemacht da Dritte auf IKT-Endgeräte im Bereich der ambulanten Versorgung zugreifen können.

6.2 Änderung der Randbedingungen

Momentan viel zu wenig IT-Sicherheit bei Medizinprodukten, Voraussetzungen für die Zulassung würde die Qualität der IT-Sicherheit solcher Produkte fördern. Zum Beispiel ein Nachweis der verwendeten Sicherheitsstandards. Eventuell eine zusätzliche Zertifizierung wäre denkbar. Außerdem muss auf die verschiedenen Risikoklassen der Medizinprodukte eingegangen werden, und, dass wenn ein Update eingespielt wird, dass derjenige nicht automatisch zum Hersteller des Medizinproduktes werden

Stationäre Versorgung: Es sollten nun die Kriterien definiert werden, welche kritische Betreiber charakterisieren und die Basis für Selbst-Audits der Leistungserbringer bilden. Die Kriterien sollten sowohl Versorgungskennzahlen und Schwellwerte festlegen, als auch Aspekte wie die individuelle IT-Durchdringung einzelner Häuser berücksichtigen, da eine kritische Abhängigkeit von IT nicht in allen Einrichtung gegeben ist.

Ambulante Versorgung: Es sind voraussichtlich keine unmittelbaren Aktivitäten notwendig, da im Rahmen dieser Studie keine kritischen Betreiber und nur eine geringe IT-Abhängigkeit identifiziert

wurden. Gegebenenfalls ist zu prüfen, ob große MVZ existieren, welche beispielsweise regional bedeutsam sind.

Arzneimittel und Impfstoffe: Es sollte mit Hilfe von Selbst-Audits der Betreiber geprüft werden, ob wichtige Wirkstoffe exklusiv in bestimmten Produktionsstätten hergestellt werden und ob sich daraus Risiken ergeben.

Labore: Auch hier sollten Kriterien für die Durchführung von Selbst-Audits durch Betreiber definiert werden, welche insbesondere die regionale Verteilung von Proben und Arbeitsschritten in Labornetzwerken stärker beleuchten.

Medizintechnik: Da es sich nicht um eine Branche im Sinne des IT-Sicherheitsgesetzes handelt, sind formal keine Aktivitäten für die Hersteller von Medizintechnik im Rahmen der KRITIS-Verordnung notwendig. Die Betreiber von Medizintechnik insb. in den Branchen medizinische Versorgung und Labore sind freilich im Fokus der KRITIS-Verordnung.

Prinzipiell besteht bei den Selbst-Audits natürlich die Problematik, dass die Angaben nicht unmittelbar überprüft werden können.

Überprüfung der KRITS Verordnung nach zwei bei drei Jahren

Ein Budget für Krankenhäuser soll vom BMG zu Verfügung gestellt werden, damit diese ihre IT-Sicherheit ausbauen, um die Anzahl der schädlichen Vorfälle in der IT vermindern soll, außerdem sollen Unternehmen in der Privatwirtschaft auch einen Anreiz bekommen die Sicherheit ihrer Produkte zu erhöhen.

6.3 Notwendige Schritte zur Umsetzung der Vorgaben aus dem IT-Sicherheitsgesetz

Um einer ablehnenden Haltung gegenüber dem „IT-Sicherheitsgesetz“ entgegenzusteuern, werden folgende Schritte empfohlen:

- Aufforderung zur aktiven Mitgestaltung der Umsetzung des IT-Sicherheitsgesetzes an die Branchen. Es muss Verständnis für die Relevanz von IT-Sicherheit geschaffen werden.
- Es soll die Gründung eigener Branchenarbeitskreise oder die Teilnahme an bereits existierenden Kreisen erfolgen.
- Es besteht die Aufgabe der Intensivierung der Arbeit im bereits existierenden Branchenarbeitskreis, insbesondere zur Entwicklung und Umsetzung von Branchenstandards
- Das BMI sowie das BSI sollten kurzfristig die Kommunikation zur Schaffung von Transparenz bezüglich des weiteren Vorgehens und der Auswahlkriterien der kritischen Betreiber intensivieren

6.4 Weiterer Forschungsbedarf

Die Digitalisierung und die steigende Vernetzung führen dazu, dass sich IT-Abhängigkeit und IT-Sicherheit sehr schnell verändern können.

Überprüfung des aktuellen Branchenschnitts im KRITIS-Sektor Gesundheit

- Soll stationäre Versorgung als eigene Branche abgetrennt von Ambulanz betrachtet werden?
- Laboranalytik eigene Branche?
- Versorgung mit Medizintechnik eigene Branche?

Neubewertung der IT-Sicherheit der ambulanten Versorgung

- Durch die Vernetzung Entstehen neue Möglichkeiten aber auch Risiken
- Außerdem sollten die vorhandenen Bestandsnetze auf IT-Sicherheit überprüft werden

Feinanpassung der MIKI-Methodik auf das Gesundheitssystem

- Methodik wird in allen Sektoren verwendet und könnte für das heterogene und stark fragmentierte Gesundheitssystem speziell angepasst werden

Vertiefende Analyse des Bereiches Medizintechnik

- Medizinprodukte sind ein sehr breites Spektrum und sollten zur Analyse in Gruppen eingeteilt werden

Sektor- und branchenübergreifender Abstimmungsbedarf

- Mögliche Bedrohungsszenarien und verwendete Standards und Best-Practices
- Aufbau eines kontinuierlichen Dialogformats „IT-Sicherheit im Gesundheitswesen“

Aktualisierung ausgewählter Studieninhalte durch das BSI

- externe Validierung der Ergebnisse in drei bis fünf Jahren
    - Grundstruktur des Gesundheitssystems und Versorgungsdienstleitungen werden sich kaum ändern
    - IKT-Abhängigkeiten der kritischen Versorgungsprozesse werden sich auf Grund der Weiterentwicklung signifikant verändern
    - Kritikalitätsabschätzung der führenden Unternehmen wird eine neue Analyse der Datenlage und Kennzahlen benötigen. Die Logik bleibt jedoch gleich.
    - Vorfallsammlung muss aktualisiert werden
    - Regulatorische Vorgaben, relevante Standards, Best-Practices und Stand der Cyber-Sicherheit müssen in den einzelnen Branchen aktualisiert werden.

Gesundheitssektor zwar relativ gering bedroht und die Sicherheitslücken noch nicht aufgedeckt bzw. noch nicht ausgenutzt, aber IT muss trotzdem professionalisiert und das IT-Sicherheitsgesetz durchgesetzt werden um Sicherheit auch in der Zukunft zu gewährleisten.