DEUTSCHE KRANKENHAUS GESELLSCHAFT

Erhebung der Kosten zur Umsetzung des IT-Sicherheitsgesetzes in BSI-KritisV-relevanten Krankenhäusern

Kostenerhebung im Auftrag und in Zusammenarbeit mit der Deutschen Krankenhausgesellschaft e. V.

Version: 2.0

Stand: 22. Oktober 2019

Hauptauftragnehmer	*Projektberatung*
Goldmedia GmbH Strategy Consulting **Prof. Dr. Klaus Goldhammer** **Dr. André Wiegand** Oranienburger Straße 27 10117 Berlin www.Goldmedia.com	**Sec2do GmbH** **Martin Peters** Uhlandstr. 28 10719 Berlin www.sec2do.com

Disclaimer

Alle Inhalte des Dokuments wurden nach bestem Wissen recherchiert und erstellt. Für Irrtümer und Druckfehler kann der Herausgeber jedoch keine Verantwortung oder Haftung übernehmen.

Der Herausgeber übernimmt keinerlei Verantwortung oder Haftung für Handlungen, Aktivitäten oder Unterlassungen, die auf Grundlage der Inhalte und Empfehlungen dieser Studie erfolgen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Alle hier genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer.

Inhalt

1 Vorwort des Auftraggebers: IT-Sicherheit im Krankenhaus

Die Gesellschaft erwartet eine 24-stündige Verfügbarkeit medizinischer Leistungen an 365 Tagen im Jahr – hierfür stehen die Krankenhäuser in Deutschland ein. Dabei spielt die zunehmende Digitalisierung im Gesundheitswesen auch im Krankenhaus eine immer stärkere Rolle. Die Anforderungen an die Sicherstellung der Verfügbarkeit, Integrität und Vertraulichkeit der im Behandlungsprozess genutzten Daten nehmen zu, je mehr die Digitalisierung den Klinikalltag mitbestimmt. Der Patient kann zu Recht erwarten, dass die ihn betreffenden Daten im Behandlungskontext zur Verfügung stehen und dabei zu jeder Zeit gegen unerlaubte Zugriffe oder Manipulationen geschützt sind. Klinikweite Systemausfälle, z.B. infolge eines einzigen "digitalen Nadelstichs" in Form einer mit Malware versehenen E-Mail, müssen verhindert werden.

Mit dem IT-Sicherheitsgesetz (ITSG) hat der Gesetzgeber Vorgaben für die Betreiber sogenannter Kritischer Infrastrukturen erlassen, die dem Schutz der dort genutzten Prozesse und Systeme dienen. Im Ergebnis sollen Dienstleistungen, die gesamtgesellschaftliche Relevanz besitzen, besser gegen Ausfälle und Manipulationen abgesichert werden. Versorgen Krankenhäuser 30.000 oder mehr vollstationäre Patientenfälle im Jahr, fallen sie gem. der BSI-Kritis-Verordnung (BSI-KritisV) unter die entsprechenden Regelungen des IT-Sicherheitsgesetzes.

Zur Verbesserung der IT-Sicherheit in den Krankenhäusern hat die Deutsche Krankenhausgesellschaft einen **branchenspezifischen Sicherheitsstandard ("B3S")** erarbeitet, und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Prüfung vorgelegt, ob die darin enthaltenen Maßnahmen zur Umsetzung der Anforderungen des § 8a BSIG geeignet sind. Diese Eignung hat das BSI am 22.10.2019 festgestellt.

Der vorgelegte Sicherheitsstandard beschreibt eine Vielzahl an Maßnahmen, um die Prozesse und Systeme, die an der Versorgung der Patienten beteiligt sind, zu schützen und die IT-Sicherheit in den deutschen Krankenhäusern zu verbessern. Ziel ist die Gewährleistung der Verfügbarkeit, Integrität und Vertraulichkeit von Informationen im Krankenhaus, unter besonderer Berücksichtigung der branchenspezifischen Gefährdungslage.

Es wird erwartet, dass durch die Umsetzung dieser im B3S definierten Maßnahmen relevante Mehrkosten für die BSI-KritisV-relevanten Krankenhäuser entstehen. Die vorliegende Studie ermittelt **die mit der Umsetzung entstehenden Kosten mit Blick auf Investitionen, Betriebskosten und Personalbedarf** auf Basis der im B3S definierten Maßnahmen.

Krankenhäuser, die im Jahr 2019 den Regelungen der BSI-KritisV unterfallen, werden infolge der Umsetzung der im B3S erarbeiteten Maßnahmen mit initialen Mehrkosten in der Größenordnung von **ca. 1,5-2,0 Mio. EUR** rechnen müssen. Im laufenden Betrieb werden, insbesondere aufgrund des erhöhten Personalbedarfs, Mehrkosten in Höhe von **ca. 500-600 TEUR pro Jahr** entstehen, die nicht in den bisher kalkulierten Budgets für Informationstechnik enthalten sind.

Mit der vorliegenden Studie können die entstehenden Kosten den einzelnen Maßnahmenblöcken zugeordnet und so eine Abschätzung des in der Umsetzung zu erwartenden Ressourcenaufwandes getroffen werden.

2 Methodensteckbrief

Die Kostenerhebung wurde von Goldmedia auf Basis folgender methodischer Grundlagen durchgeführt:

- **Art der Befragung**:
  Quantitative Online-Befragung der BSI-KritisV-relevanten Krankenhäuser
- **Feldzeit:** 13.12.2018 bis 07.02.2019
- **Grundgesamtheit:** 212 BSI-KritisV-relevante Krankenhäuser *(Abgrenzung des erhebungsrelevanten Krankenhaussegments auf Basis der Qualitätsberichte des Gemeinsamen Bundesausschusses mit mindestens 29.000 vollstationären Fällen/Jahr)*
- **Ansprache:** Einladung zur Online-Erhebung per E-Mail mit individualisiertem, passwortgeschütztem Zugang an alle Häuser der Grundgesamtheit. Erinnerungsmail nach 4 Wochen an alle Krankenhäuser mit bis dato unvollständigem bzw. fehlendem Erhebungsbogen.
- **Teilnehmer:** n=62 gültige Fragebögen (29,2 Prozent der Grundgesamtheit)
  - davon 50 Häuser oberhalb des BSI-KritisV-Schwellwerts
    (entspricht 23,6 Prozent der Grundgesamtheit)
  - sowie 12 Häuser unterhalb des BSI-KritisV-Schwellwerts
- **Abdeckungsgrad der Teilnehmer an der Gesamtversorgung:**
  - entspricht min. 204 Einzel-Standorten
  - entspricht min. 3,2 Mio. vollstationären Fällen/Jahr
- **Durchschnittliche Bearbeitungszeit (brutto) der Teilnehmer:**
  207 Stunden pro Erhebungsbogen
- **Median-Bearbeitungszeit (brutto) der Teilnehmer**:
  50 Stunden pro Erhebungsbogen

3 Kernergebnisse der Kostenerhebung

- Hohe Beteiligung an der Erhebung (n=62 gültige Fragebögen, 28,8 Prozent der Grundgesamtheit) trotz besonders hoher Befragungskomplexität (Ausfüllzeit-Median: 50 Stunden)
- Median-Krankenhaus innerhalb der BSI-KritisV-relevanten Stichprobe:
  2 Standorte, ~1.000 Betten, ~38.000 vollstationäre Fälle/Jahr
- Eine **Hochrechnung der zusätzlichen Kosten durch Maßnahmen zur Umsetzung des B3S** im BSI-KritisV-relevanten Segment ist mithilfe der Erhebung möglich, da die Analyse eine starke Korrelation zwischen Kosten und vollstationären Fällen/Jahr ergab.

Die Modellierung des BSI-KritisV-relevanten Krankenhaussegments aus **N=154 Krankenhäusern** ergibt folgende **Gesamtkosten** für die Umsetzung der Maßnahmen aus dem B3S:

Tab. 1: Hochrechnung der zusätzlichen Kosten durch Maßnahmen zur Umsetzung des B3S im BSI-KritisV-relevanten Segment, in Mio. EUR

	Summe	IT	Facility-Management	Sicherheits-Management	Verwaltung	Medizin-Technik	Einkauf
	in Mio. EUR						
1. Jahr	**532**	355	67	51	41	12	5
Folgejahre	**231**	106	20	47	39	15	5

Quelle: Goldmedia Analyse 2019, Modellannahme: N=154 Krankenhäuser mit insgesamt 6,7 Mio. vollstationären Fällen/Jahr. Basis: Kostenangaben von n=62 Krankenhäusern.

Die Median-Ergebnisse zeigen zudem die Kosten für die Umsetzung der Maßnahmen aus dem B3S für jedes der BSI-KritisV-relevanten Krankenhäuser:

Tab. 2: Zusätzliche Kosten durch Maßnahmen zur Umsetzung des B3S in einem typischen BSI-KritisV-relevanten Krankenhaus, in Tsd. EUR

	Summe	IT	Facility-Management	Sicherheits-Management	Verwaltung	Medizin-Technik	Einkauf
	in Tsd. EUR						
1. Jahr	**3.006**	2.007	380	289	234	67	28
Folgejahre	**1.303**	598	111	263	218	82	30

Quelle: Goldmedia Analyse 2019, Median-Krankenhaus innerhalb des BSI-KritisV-relevanten Segments mit 38.000 vollstationären Fällen/Jahr. Basis: Kostenangaben von n=62 Krankenhäusern.

4 Hochrechnung der zusätzlichen Kosten durch Maßnahmen nach B3S für die BSI-KritisV-relevanten Krankenhäuser

4.1 Methodik der Hochrechnung

Abgrenzung der BSI-KritisV-relevanten Krankenhäuser:

- Die Grundgesamtheit umfasst N=154 Krankenhäuser, basierend auf einer Fallzahl von mindestens 29.000 vollstationären Fällen pro Haus und Jahr gemäß der Qualitätsberichte des Gemeinsamen Bundesausschusses. Der abgegrenzte Markt umfasst insgesamt 6,73 Mio. vollstationäre Fälle/Jahr.

- Der Schwellwert 29.000 vollstationäre Fälle/Jahr wurde gewählt, um der Tatsache Rechnung zu tragen, dass die BSI-KritisV auch für solche Krankenhäuser hohe Relevanz besitzt, die den Schwellwert bislang nicht erreichen, aber mittelfristig unter das Regime der BSI-KritisV fallen könnten.

Hochrechnung der BSI-KritisV-relevanten Krankenhäuser:

- Die Hochrechnung basiert auf den erhobenen durchschnittlichen Einzelkostenpositionen der Krankenhäuser innerhalb der Stichprobe (n=62), bezogen auf 10.000 vollstationäre Fälle/Jahr.

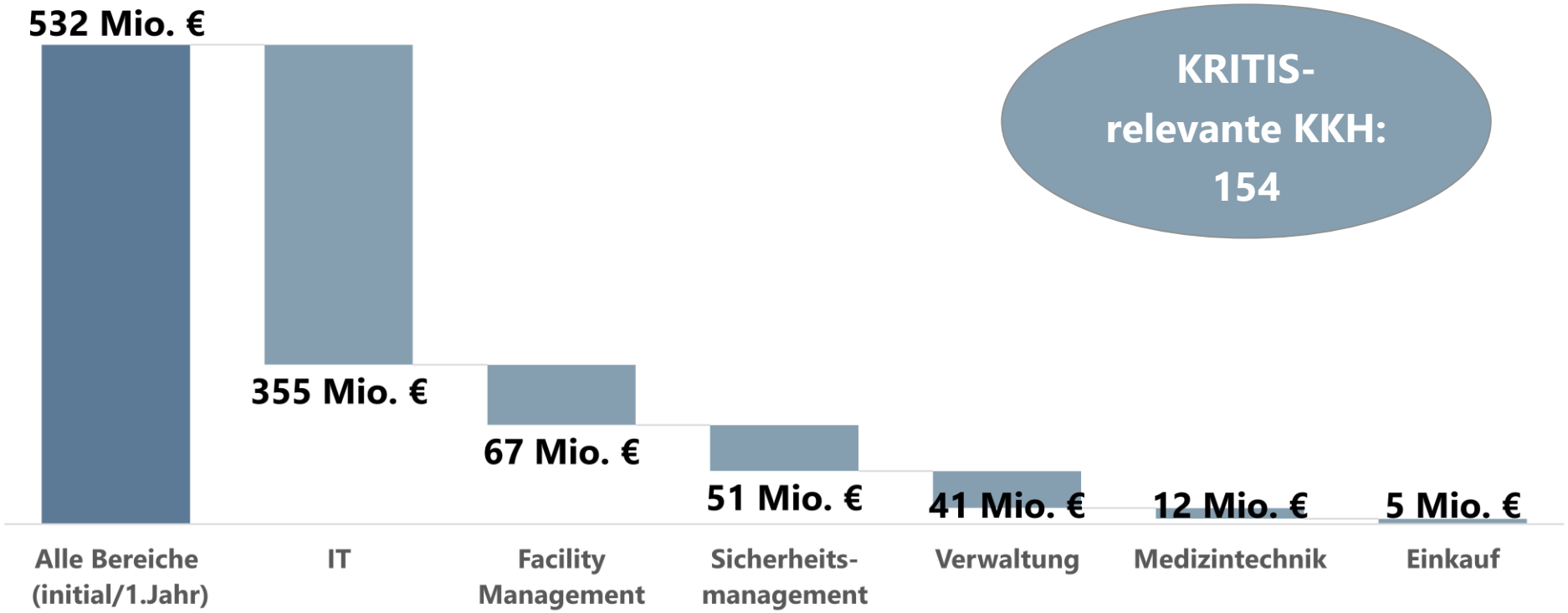
- Diese Basis würde gewählt, da eine **hohe Korrelation zwischen der Anzahl vollstationärer Fälle/Jahr und den empirisch erhobenen Gesamtkosten** besteht.

- Antwortausfälle in den Erhebungsbögen (Kostenpositionen ohne Angaben) wurden um die erhobenen Durchschnittswerte der jeweiligen Kostenpositionen ergänzt (imputiert), um die Hochrechnung auf Basis der Gesamtstichprobe (n=62 Krankenhäuser) zu ermöglichen.

- Hieraus wurden die Summe der zusätzlichen Kosten durch IT-Sicherheitsmaßnahmen infolge der Umsetzung des B3S für das BSI-KritisV-relevante Segment der deutschen Krankenhäuser (N=154) hochgerechnet.

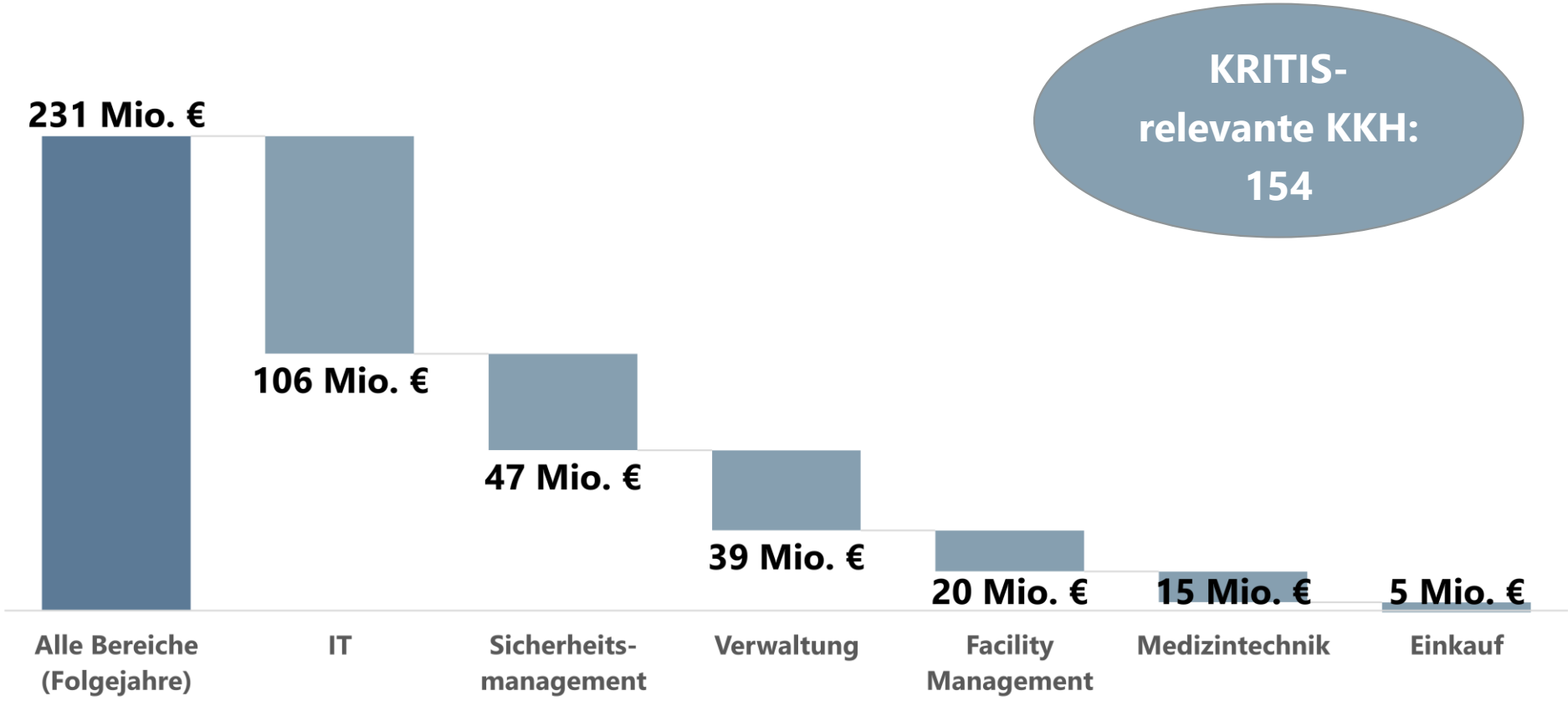
- Die erhobenen Durchschnittswerte jeder einzelnen Kostenposition (dargestellt in der Einheit „pro 10.000 vollstationäre Fälle/Jahr“) wurden dafür mit den aggregierten vollstationären Fällen/Jahr der abgegrenzten, BSI-KritisV-relevanten Krankenhäuser multipliziert (N=154 Krankenhäuser mit in Summe 6,73 Mio. vollstationären Fällen/Jahr).

4.2 Initiale Kosten im 1. Jahr für 154 BSI-KritisV-relevante Krankenhäuser, in Mio. EUR



Annahme: Zusätzliche Kosten infolge der Umsetzung der Maßnahmen des B3S entstehen für BSI-KritisV-relevante Krankenhäuser (N=154 Krankenhäuser mit mindestens 29.000 stationären Fällen pro Jahr).
Quelle: Goldmedia Analyse 2019

4.3 Wiederkehrende Kosten für 154 BSI-KritisV-relevante Krankenhäuser, in Mio. EUR/Jahr



Annahme: Zusätzliche Kosten infolge der Umsetzung der Maßnahmen des B3S entstehen für BSI-KritisV-relevante Krankenhäuser (N=154 Krankenhäuser mit mindestens 29.000 stationären Fällen pro Jahr).
Quelle: Goldmedia Analyse 2019

5 Zusätzliche Kosten infolge der Umsetzung der Maßnahmen des B3S

5.1 Kostenüberblick

- Die einzelnen Kostenpositionen der Befragung wurden für die zusammenfassende Darstellung zu Teilbereichen (nach sowohl initialen als auch wiederkehrenden Kosten) aufsummiert.
- Fehlende Werte des Rohdatensatzes wurden hierfür auf Basis der erhobenen Durchschnittswerte (je zugrunde liegender Kostenposition) imputiert.

Im Ergebnis wurden folgende Kosten auf **10.000 vollstationäre Fälle/Jahr** vereinheitlicht, um eine Vergleichbarkeit herzustellen:

Tab. 3: Zusätzliche Kosten infolge der Umsetzung der Maßnahmen des B3S in EUR pro 10.000 vollstationäre Fälle/Jahr

Bereich innerhalb des Krankenhauses	Gültige N*	Zusätzliche Kosten (je 10.000 vollst. Fälle) in EUR
Teilbereich Sicherheitsmanagement initial/1.Jahr	62	76.033
Teilbereich Sicherheitsmanagement Folgejahre	62	69.153
Teilbereich IT initial/1.Jahr	62	528.228
Teilbereich IT Folgejahre	62	157.368
Teilbereich Medizintechnik initial/1.Jahr	62	17.661
Teilbereich Medizintechnik Folgejahre	62	21.584
Teilbereich Einkauf initial/1.Jahr	62	7.422
Teilbereich Einkauf Folgejahre	62	8.139
Teilbereich Facility Management initial/1.Jahr	62	99.981
Teilbereich Facility Management Folgejahre	62	29.272
Teilbereich Verwaltung initial/1.Jahr	62	61.680
Teilbereich Verwaltung Folgejahre	62	57.369
Alle Bereiche: Kosten initial	**62**	**791.005**
Alle Bereiche: Kosten Folgejahre	**62**	**342.885**

** Gültige N: Anzahl der Befragungsteilnehmer mit Angaben zu Kosten und stationären Fällen/Jahr.*

Quelle: Goldmedia Analyse 2019

5.2 Detaildarstellung der erhobenen Kosten

Erläuterungen zu den Begrifflichkeiten der Detail-Auswertungen:

- Valid/Gültige N = absolute Anzahl der Befragungsteilnehmer pro Frage
- Mean = Arithmetischer Mittelwert der gültigen Befragungsteilnehmer
- Minimum = geringster Wert in der Stichprobe
- Percentile 25 = unteres Quartil (25% der Werte in der Stichprobe liegen darunter)
- Median = Zentralwert (50% der Werte in der Stichprobe liegen darunter)
- Percentile 75 = oberes Quartil (75% der Werte in der Stichprobe liegen darunter)
- Maximum = höchster Wert in der Stichprobe
- Sum = Summe aller Werte in der Stichprobe

Tab. 4: Erhobene[1] initiale Kosten und Folgekosten [pro 10.000 vollstationäre Fälle/Jahr], in EUR

	Valid N	Mean	Min	Perc. 25	Median	Perc. 75	Max	Sum
Anzahl der Standorte	58	4	1	1	2	4	61	208
Anzahl der Mitarbeiter	57	4.580	455	1.900	2.600	5.602	36.000	261.086
Anzahl der Betten	62	1.405	350	700	955	1.400	19.000	87.090
Anzahl vollstationärer Fälle	62	57.098	7.100	31.275	39.196	55.405	693.000	3.540.095
Teilbereich Sicherheitsmanagement								
Personalkosten (initial)	54	25.335	0	11.765	18.928	33.798	140.845	
Personalkosten (Folgejahre)	56	31.304	2.802	13.108	22.897	38.924	225.352	
Zusätzliche Beratungsleistungen: Betriebskosten (initial)	57	16.639	0	5.490	14.167	21.659	70.423	
Zusätzliche ext Schulungen/Weiterbildungen ISM-Team: Betriebsk. (initial)	56	3.748	0	1.657	3.376	4.993	14.085	
Zusätzliche Beratungsleistungen: Betriebskosten (Folgejahre)	55	11.826	0	3.324	6.760	11.824	87.719	
Zusätzliche ext Schulungen/Weiterbildungen ISM-Team: Betriebsk. (Folgejahre)	53	3.728	0	1.182	1.951	3.913	49.669	
Zusätzliche Arbeitsmittel: Investitionskosten (initial)	54	30.312	0	2.852	12.060	22.125	397.351	
Zusätzliche Arbeitsmittel: Betriebskosten (Folgejahre)	54	22.295	0	1.250	2.328	6.314	827.815	

[1] *Keine Imputation fehlender Werte innerhalb der Rohdaten. Die Zahl gültiger Antworten unterscheidet sich daher zwischen den Kostenpositionen.*

Teilbereich Informationstechnik (IT)							
Personalkosten (initial)	59	31.487	0	12.213	20.548	34.293	340.845
Personalkosten (Folgejahre)	59	38.884	0	11.544	20.000	39.077	597.183
ext Schulungen/Weiterbildungen IT-Mitarbeiter: Schulungskosten (initial)	56	6.628	0	1.821	4.621	7.449	70.423
ext Schulungen/Weiterbildungen IT-Mitarbeiter: Schulungskosten (Folgejahre)	55	6.239	0	1.429	3.608	6.849	70.423
Robuste/resiliente Architektur Investitionskosten	48	210.017	0	14.758	55.185	146.792	3.570.086
Netzsegmentierung Investitionskosten	53	60.396	0	5.604	17.866	42.779	946.342
Firewall Investitionskosten	56	35.187	0	7.317	18.550	47.253	225.479
Schutz vor Schadsoftware Investitionskosten	57	17.869	0	4.783	8.571	18.750	126.761
Härtung der Basiskonfiguration Investitionskosten	45	12.592	0	1.778	5.556	12.628	157.746
Systemgestützte Protokollierung und Protokollauswertung Investitionskosten	49	17.751	0	2.439	7.260	15.894	169.014
Einsatz von Intrusion Detection/ Prevention- Systemen: Investitionskosten	53	13.773	0	2.745	9.091	20.522	50.714
Authentisierung Investitionskosten	51	21.193	0	3.750	8.846	37.143	98.013
Mobile Device Management Investitionskosten	54	15.230	0	3.125	8.199	15.987	187.899
Verschlüsselung von Festplatten und E-Mail- Kommunikation Investitionskosten	52	12.969	0	1.694	6.264	17.490	156.000
Datensicherung und Archivierung Investitionskosten	50	38.255	0	7.143	19.554	37.255	530.831
Trennung/Härtung v. Test/Betriebs-Umgebungen (Gesundheitsdaten) Invest.	42	28.801	0	4.878	10.216	24.706	485.915
Sichere Löschung, Entsorgung, Ausmusterung Investitionskosten	39	6.080	0	1.081	2.333	5.000	74.503
Robuste/resiliente Architektur Betriebskosten	44	42.784	0	3.318	7.745	22.188	714.017
Netzsegmentierung Betriebskosten	49	12.024	0	1.042	4.110	10.000	204.225
Firewall Betriebskosten	54	8.333	0	1.923	5.303	10.372	49.296
Schutz vor Schadsoftware Betriebskosten	55	6.304	433	1.599	3.030	7.671	42.254
Härtung der Basiskonfiguration Betriebskosten	47	3.732	0	662	1.662	3.197	53.521
Systemgestützte Protokollierung und Protokollauswertung Betriebskosten	48	4.930	0	718	2.026	4.750	56.338
Einsatz von Intrusion Detection/ Prevention- Systemen: Betriebskosten	50	3.461	0	707	2.163	4.736	20.833
Authentisierung Betriebskosten	50	4.251	0	709	2.166	5.970	21.523
Mobile Device Management Betriebskosten	53	3.669	0	1.143	1.837	3.157	37.580
Verschlüsselung von Festplatten und E-Mail- Kommunikation Betriebskosten	49	3.906	0	707	1.569	4.500	31.200
Datensicherung und Archivierung Betriebskosten	49	8.288	0	1.566	3.425	8.309	106.201

Trennung/Härtung v. Test/Betriebs-Umgebungen (Gesundheitsdaten) Betriebsk.	42	7.580	0	1.089	2.483	5.714	161.972	
Sichere Löschung, Entsorgung, Ausmusterung Betriebskosten	43	2.981	0	560	1.312	3.197	21.127	
Teilbereich Medizintechnik								
Personalkosten (initial/1.Jahr)	44	17.661	0	3.145	11.587	18.542	253.521	
Personalkosten (Folgejahre)	44	21.584	0	2.606	10.250	18.258	422.535	
Teilbereich Einkauf								
Personalkosten (initial/1.Jahr)	40	5.999	0	1.110	3.748	9.310	42.254	
Personalkosten (Folgejahre)	40	6.800	0	1.110	3.296	9.310	47.145	
Schulungskosten (initial/1.Jahr)	38	1.423	0	446	1.194	1.662	5.000	
Schulungskosten (Folgejahre)	38	1.338	0	285	625	1.556	14.144	
Teilbereich Facility Management								
Personalkosten (initial)	39	8.060	0	2.740	6.087	12.500	23.573	
Personalkosten (Folgejahre)	39	8.094	0	2.500	5.955	11.429	47.145	
Physische Sicherheit/ Gebäudesicherheit Investitionskosten	45	87.989	0	8.108	23.647	109.130	1.375.000	
Betriebliche Entsorgung Investitionskosten	33	3.932	0	522	2.055	4.615	27.397	
Physische Sicherheit/ Gebäudesicherheit Betriebskosten	42	17.369	0	1.304	5.257	20.000	208.333	
Betriebliche Entsorgung Betriebskosten	32	3.809	0	511	1.870	4.699	27.397	
Teilbereich Fach- und Funktionsabteilungen/Verwaltung								
Personalkosten (initial)	36	43.109	0	5.635	9.983	20.221	466.667	
Personalkosten (Folgejahre)	37	43.049	0	4.706	11.667	27.778	466.667	
Schulungskosten (initial/1.Jahr)	38	18.571	0	833	1.571	5.556	354.167	
Schulungskosten (Folgejahre)	37	14.320	0	435	1.429	10.000	354.167	

[1] *Keine Imputation fehlender Werte innerhalb der erhobenen Rohdaten. Die Zahl gültiger Antworten kann sich daher zwischen den einzelnen Kostenpositionen unterscheiden.*
Quelle: Goldmedia Analyse 2019