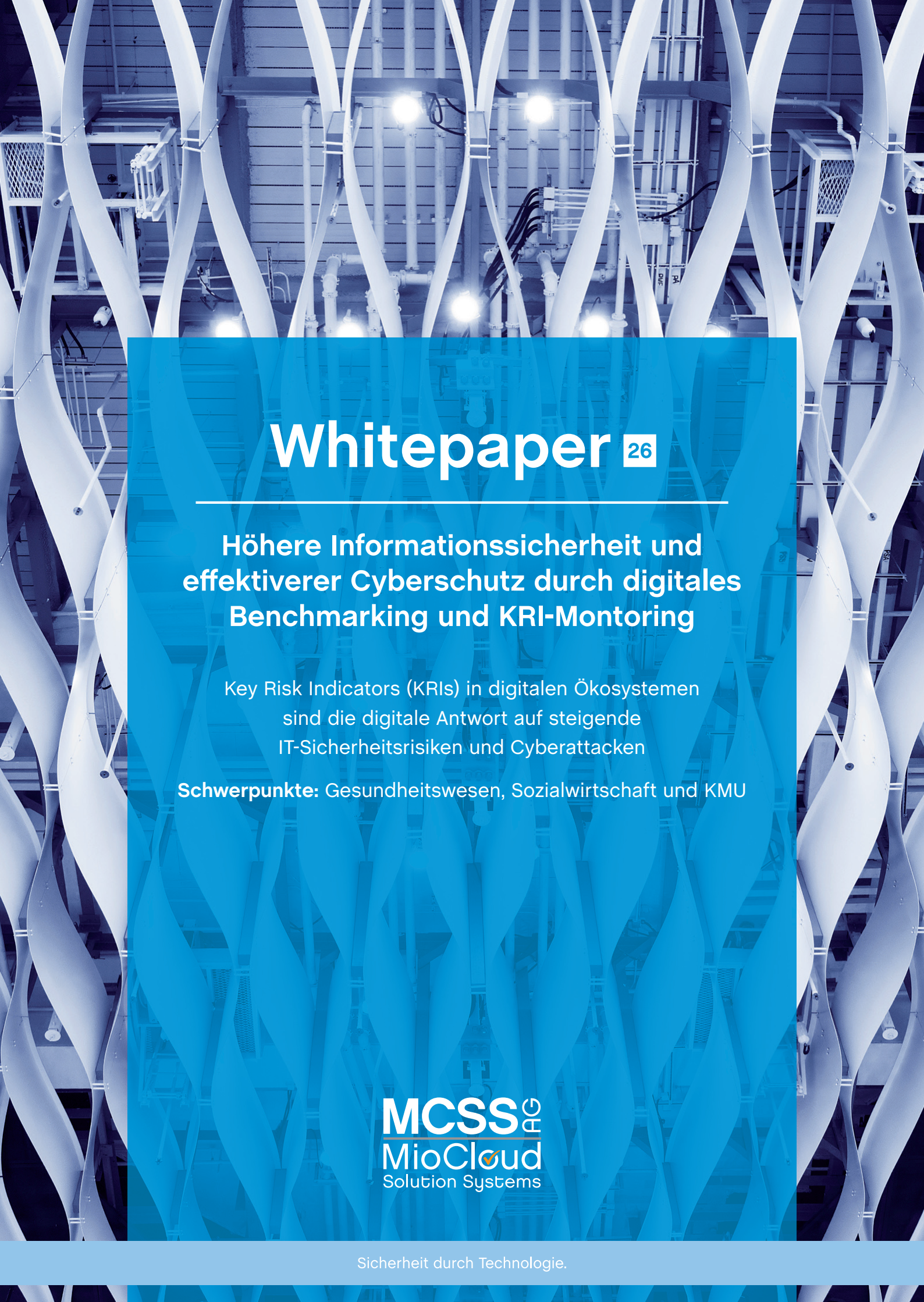


Whitepaper 26

Höhere Informationssicherheit und effektiverer Cyberschutz durch digitales Benchmarking und KRI-Montoring

Key Risk Indicators (KRIs) in digitalen Ökosystemen sind die digitale Antwort auf steigende IT-Sicherheitsrisiken und Cyberattacken

Schwerpunkte: Gesundheitswesen, Sozialwirtschaft und KMU

MCSS AG
MioCloud
Solution Systems

Sicherheit durch Technologie.

INHALT

1 Extrakt 4

2 Definition und Aufgabenbereiche 5

2.1 IT-Sicherheit 5
2.2 Informationssicherheit 5
2.3 Cyber-Sicherheit 5
2.4 Benchmarking und Key Indicators 6

3 Benchmarking und digitale Kennzahlen 7

3.1 Key Risk Indicators (KRI) 7
3.2 Key Performance Indicators (KPI) 8
3.3 Die Beziehung zwischen KPIs und KRIs 8
3.4 Indikatoren im Gesundheitswesen: Digitale Reifegradmessung 9

4 Informationssicherheits-Ausschöpfungskennzahl (ISAK) 10

4.1 Datapoints nach GDV Fragenkatalog für Cyber-Versicherer 11
4.2 ISAK im Gesundheitswesen und in der Sozialwirtschaft 12
4.3 ISAK in kleinen und mittleren Unternehmen (KMU) 14
4.4 Historie und Zukunft von ISAK 16
4.4.1 Historie der Entwicklung 16
4.4.2 Forschungsprojekte 16
4.5 Beispiele zur Nutzung von Benchmarks im Informationssicherheits- und Datenschutzmanagement 17

5 Handlungsempfehlungen 19

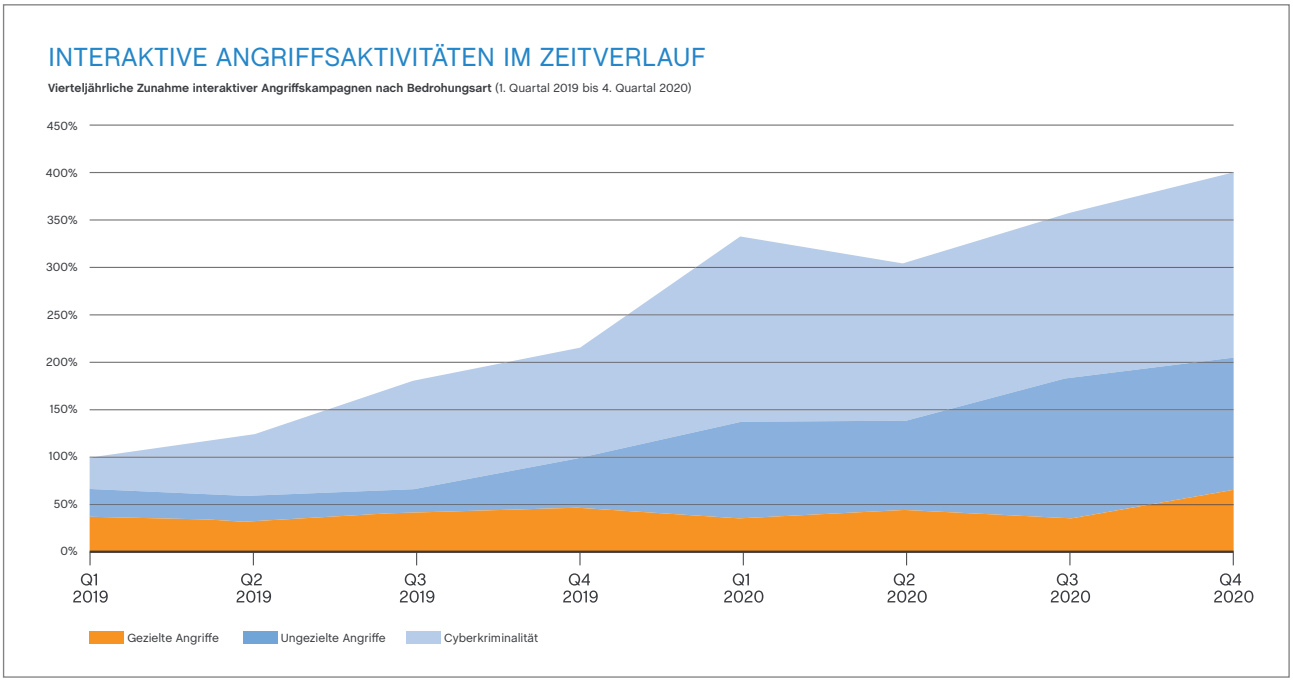
6 Zusammenfassung 19

7 Die Autoren 20

8 Referenzen/Anlagen 22

1 Extrakt

Die Berichte über Cyberangriffe nehmen national und international zu. Damit steigen die Risiken für IT-Ausfälle mit Betriebsunterbrechungen erheblich.



Die Vervierfachung der Angriffe in nur 2 Jahren macht die steigende Cybergefahr deutlich. Die ungezielten Angriffe (also Attacken mit zufälligen Zielen) können jede Organisation treffen. Der Cyberstörfall an der Universitätsklinik in Düsseldorf ist dafür ein erschreckendes Beispiel (Quelle: Global Threat Report 2021, Crowdstrike).

Die Risikoentwicklungen müssen zuerst transparent gemacht werden, um Gegenmaßnahmen und Lösungen zu entwickeln und umzusetzen. Zur Erhöhung der Risikotransparenz für Verantwortliche (und ihre Versicherer) wurden Benchmarks in Form von Key Performance Indicators (KPIs) und Key Risk Indicators (KRIs) entwickelt.

2 Definitionen und Anwendungsbereiche

2.1 IT-Sicherheit

Die IT-Sicherheit bezieht sich auf den Schutz der IT-Infrastruktur von Einrichtungen, Selbstständigen, Unternehmen, Kliniken und Krankenhäusern etc. mit dem Ziel, wirtschaftlichen Schaden und Datenschutzverstöße zu verhindern. Es finden Werkzeuge wie Antivirenprogramme, Spamfilter und Passwortmanager ihre Anwendung.

2.2 Informationssicherheit

Die Informationssicherheit beinhaltet die IT-Sicherheit, erweitert diesen Begriff jedoch um die Sicherheit von nicht technisch gespeicherten und elektronisch verarbeiteten Daten. Um das Erreichen von Informations- und IT-Sicherheit messbar zu machen, werden sogenannte Schutzziele definiert.

Allgemeine Schutzziele sind dabei:

- Die Vertraulichkeit von Daten, dass keine Daten von unberechtigten Personen gelesen oder verändert werden dürfen, beispielsweise durch Richtlinien, Nutzergruppen und der Anwendung des sogenannten Need-to-know-Prinzips (Erforderlichkeitsprinzip).
- Die Integrität von Daten, dass keine Daten unbemerkt verändert werden dürfen und jede Veränderung beispielsweise durch Logs nachvollziehbar belegt werden kann. Auch die Konsistenz von Daten, also die Abhängigkeit der Daten untereinander zählt zum Schutzziel der Integrität.
- Die Verfügbarkeit von Daten, die in definierten Zeiträumen gewährleistet sein muss (beispielsweise Aufbewahrungsfristen medizinischer Daten und Informationen). Dieses Schutzziel wird unter anderem durch das Erstellen von regelmäßigen Datensicherungen (Backups), redundanter Datenhaltung und Langzeit-Archivierung erreicht.

2.3 Cyber-Sicherheit

Die Cyber-Sicherheit wird häufig entweder der Informationssicherheit gleichgesetzt oder dieser übergeordnet. Sie beinhaltet nicht nur die Sicherheit von Daten und der IT-Infrastruktur einer einzelnen Organisation, sondern bezeichnet den Sicherheitsbegriff umfassender bis hin zur nationalen oder globalen Sicherheit. Damit ist Cyber-Sicherheit als Prozess zur Implementierung von Kontrollen zu verstehen, mit dem die Eintrittswahrscheinlichkeit von Datenschutzverletzungen aus einem Cyberangriff reduziert werden kann.

Zusammenfassung für den Bereich der medizinischen Versorgung:

- IT-Sicherheit bezieht sich auf ein soziotechnisches System, in dem Informationen mit Hilfe von Informationstechnik (IT) erfasst, gespeichert und verarbeitet werden.
- IT-Sicherheit erhält durch die Einführung der elektronischen Patientenakte (ePA) eine deutlich größere Bedeutung.

Dagegen ist Informationssicherheit umfassender definiert und umfasst auch auf Papier dokumentierte Daten und Informationen.

2.4 Benchmarking und Key Indicators

Das Gabler Wirtschaftslexikon definiert:

> *„Benchmarking ist der kontinuierliche Vergleich von Produkten, Dienstleistungen sowie Prozessen und Methoden mit (mehreren) Organisationen, um die Leistungslücke zum sog. Klassenbesten (Organisationen, die Prozesse, Methoden etc. hervorragend beherrschen) systematisch zu schließen. Grundidee ist es, festzustellen, welche Unterschiede bestehen, warum diese Unterschiede bestehen und welche Verbesserungs-möglichkeiten es gibt.“*

Im Zeitalter der Digitalisierung bekommen Benchmarks eine immer größere Rolle.
Sie werden z.B. in der Big Data Analyse und als Grundlagen für Machine Learning verwendet.

Vergleichbar mit Benchmarks sind die sogenannten „Key Indicators“.
Der Unterschied zwischen Benchmarks und Key Performance Indicators (KPI) ist, dass bei Benchmarks die eigene Performance einer Organisation oder einer Einrichtung mit der anderer verglichen wird. Im Gegensatz dazu wird mit KPI der Fortschritt in Bezug auf die Ziele einer Unternehmung oder einer Organisation gemessen.

Key Performance Indicators (KPI) oder wichtige Leistungsparameter haben eine lange Geschichte. Schon die Herrscher der chinesischen Wei Dynastie nutzten vergleichende Leistungsparameter zur Beurteilung der Familienmitglieder.

In den 1990er Jahren stellten Dr. Robert Kaplan und Dr. David Norton die „Balanced Scorecard“ vor. In diesem Kontext wurden auch die KPIs und damit kombinierbar die KRIs (Key Risk Indicators) entwickelt.

Im Jahr 2005 wurden KPIs im Qualitätsmanagement und für die Patientensicherheit in der medizinischen Versorgung vorgestellt. Auf diesen Grundlagen der PSAK (Patientensicherheit-Ausschöpfungskennzahlen) wurden die **ISAK**-Modelle (Informationssicherheit-Ausschöpfungskennzahlen) entwickelt (eingetragene Wortmarke der **MCSS AG, Köln**).

3 Benchmarking mit digitalen Kennzahlen

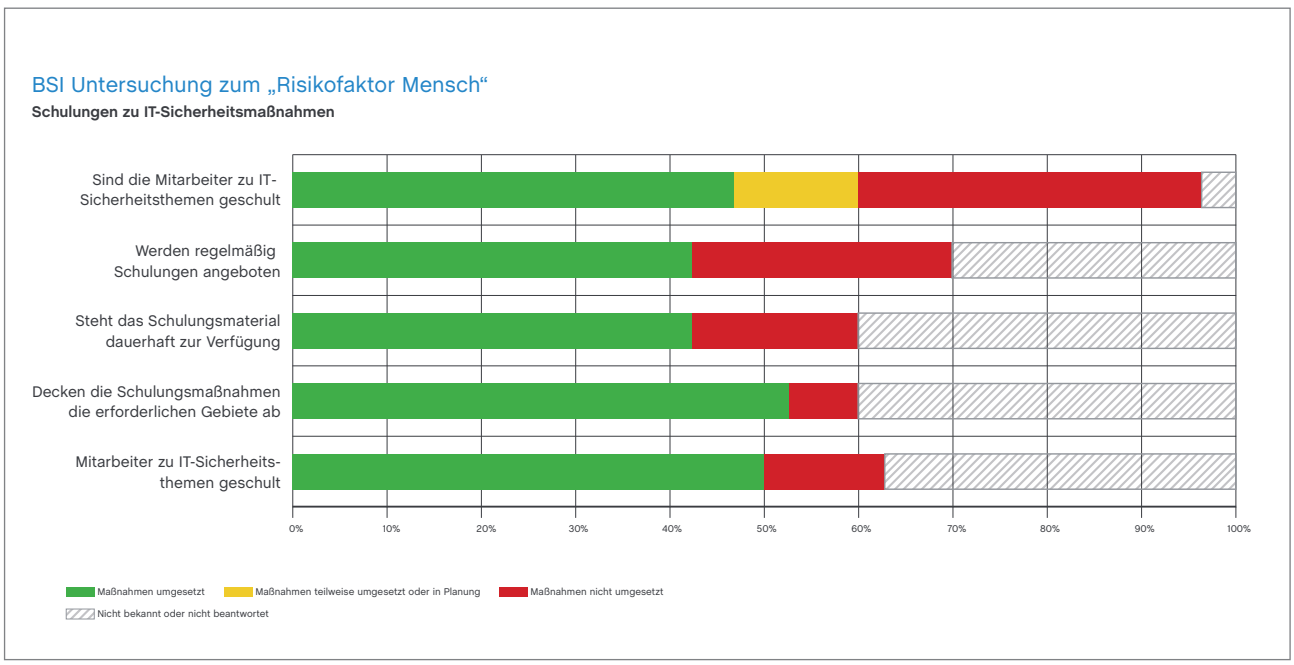
3.1 Key Risk Indicators (KRIs)

KRIs werden von Organisationen in der Informationssicherheit verwendet, um zu bestimmen, welchem Sicherheitsrisiko sie ausgesetzt sind.

KRIs sind eine Möglichkeit, die größten Risiken, denen ein Unternehmen, und speziell medizinische und soziale Versorgungseinheiten ausgesetzt sind, zu quantifizieren und zu überwachen. Durch die Messung der Risiken und ihrer potenziellen Auswirkungen auf die Sicherheit der Versorgung und der Sicherheit sind Praxen, Kliniken und Unternehmen in der Lage, Frühwarnsysteme zu schaffen, die es ihnen ermöglichen, wichtige Risiken zu überwachen, zu verwalten und zu mindern.

Effektive KRIs helfen:

- die größten IT-Risiken zu identifizieren
- diese Risiken und ihre Auswirkungen zu quantifizieren
- ermöglichen eine regelmäßige Risikoberichterstattung und Risikoüberwachung (Monitoring) intern und extern (gegenüber Versicherern)



Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI): Die Untersuchungsergebnisse machen deutlich, dass zwischen 45% bis 50% aller befragten Unternehmen nicht ausreichend auf IT-Sicherheitsmaßnamen vorbereitet sind. Mit einem KRI wie ISAK (Informationssicherheit-Ausschöpfungskennzahl) sind Lücken in der Konformität der Mitarbeiter-Qualifikation transparent erkennbar.

3.2 Key Performance Indicators (KPIs)

KPIs sind die Maßstäbe und Messungen, die eine Einrichtung verwendet, um zu verstehen, wie gut eine Organisation, im Hinblick auf ihre strategischen und sicherheitsrelevanten Ziele (Secutity Policy) abschneidet.

Sobald eine medizinische Einrichtung die Sicherheits-Ziele identifiziert hat, dienen KPIs als Überwachungs- und Entscheidungshilfen, die bei der Beantwortung der wichtigsten Leistungsfragen der Einrichtung helfen.

BSI Struktur zur KPI Messung

KPI = Key Performance Indicator

Organisation	Personal & Schulungen	Sicherheits-prozesse	Verantwort-lichkeiten	Richtlinien und Anweisungen
Technik	Infrastruktur	IT-Systeme	Netzwerke	Anwendungen
Prävention	Datensicherung	Umgang mit Sicherheits-vorfällen	Notfall-management	Aktualität der Informationen
Management	Geschäfts-prozesse	Bewertung der Gefahrenbereiche	Reifegrade	Zukunftsthemen

Quelle: BSI. Die Key Performance wird danach in den Bereichen Organisation, Technik, Prävention und Management gemessen. Die rot und gelb markierten Felder signalisieren entsprechenden Handlungsbedarf (technische und organisatorische Maßnahmen/TOM)

3.3 Die Beziehung zwischen KPIs und KRIs

Während KPIs Organisationen dabei helfen zu verstehen, wie gut sie in Bezug auf ihre strategischen Pläne abschneiden, helfen ihnen KRIs, die damit verbundenen Risiken und die Wahrscheinlichkeit, mit denen sie in Zukunft keine guten Ergebnisse zu erzielen würden, zu verstehen. Dies bedeutet, dass KRIs die Kehrseite oder KPIs sein können.

Drei Beispiele, die diesen Zusammenhang verdeutlichen:

- Eine Praxis kann einen KPI zur Messung der IT-Systemleistung und einen ergänzenden KRI zur Verfolgung der IT-Anfälligkeit für Cyberangriffe einrichten.
- Eine Praxis erstellt einen KPI, um die Patientenzufriedenheit und -sicherheit zu überwachen, da dies ein wichtiges Qualitätsziel ist. Ein mit dem gleichen Ziel verknüpfter KRI könnte die Risiken des Verlusts an Zufriedenheit der Patienten überwachen.
- Eine Praxis kann Mitarbeiterengagement oder Mitarbeiterzufriedenheit als wichtige KPIs messen und die Wahrscheinlichkeit des Verlustes wichtiger Mitarbeiter und die Risiken für seine Arbeitgebermarke als KRIs überwachen.

KPIs und KRIs sind nicht dasselbe:
KRIs helfen, Risiken zu quantifizieren, während KPIs helfen, die Versorgungsleistung zu messen.

3.4 Indikatoren im Gesundheitswesen: digitale Reifegradmessungen

Mit dem Begriff „Reifegrad“ wird die Umsetzung einer bestimmten Methode oder eines Handlungs- und Führungsmodells in der Einrichtung beschrieben. Häufig ist der Begriff „Reifegrad“ auch im Zusammenhang mit Risikomanagement, Qualitätsmanagement und anderen Managementbereichen zu finden.

Zukünftig werden KRIs und KPIs im Gesundheitswesen eine zentrale Rolle als Benchmarks für Förderungen spielen.

Das Konsortium „Digital Radar“ entwickelt ein deutsches Reifegradmodell nach § 14b Krankenhauszukunftsgesetz (KHZG), das eine internationale, standardisierte und umfassende Bewertung des Digitalisierungsgrads von Krankenhäusern ermöglichen soll. Mithilfe dieses Modells sollen Krankenhäuser zwischen dem 30. Juni und dem 30. September 2021 ihren digitalen Reifegrad messen. Zwei Jahre später erfolgt eine weitere Erhebung.

MOST WIRED DIGITALISIERUNGSGRAD MESSUNG

Segmente	Maximal mögliche Punktzahl	Prozentsatz Gesamtpunkte
Infrastruktur	44,5	9,0
Security	69,0	14,0
Administration/Beschaffungs- & Lieferkette	76,0	15,4
Analytics und Data Management	17,0	3,
Interoperabilität und Population Health	95,0	19,3
Patient Engagement	102,5	20,8
Medizinische Qualität und Patientensicherheit	66,5	13,5
Summe	**492,0**	**100,0**

Quelle: Academy of Health Information Management Executives (AHIME) (Digital Health Most Wired Survey): das KRI Modell der **MCSS AG, Köln** entspricht dem im Konsortium entwickelten Muster der Bewertung.

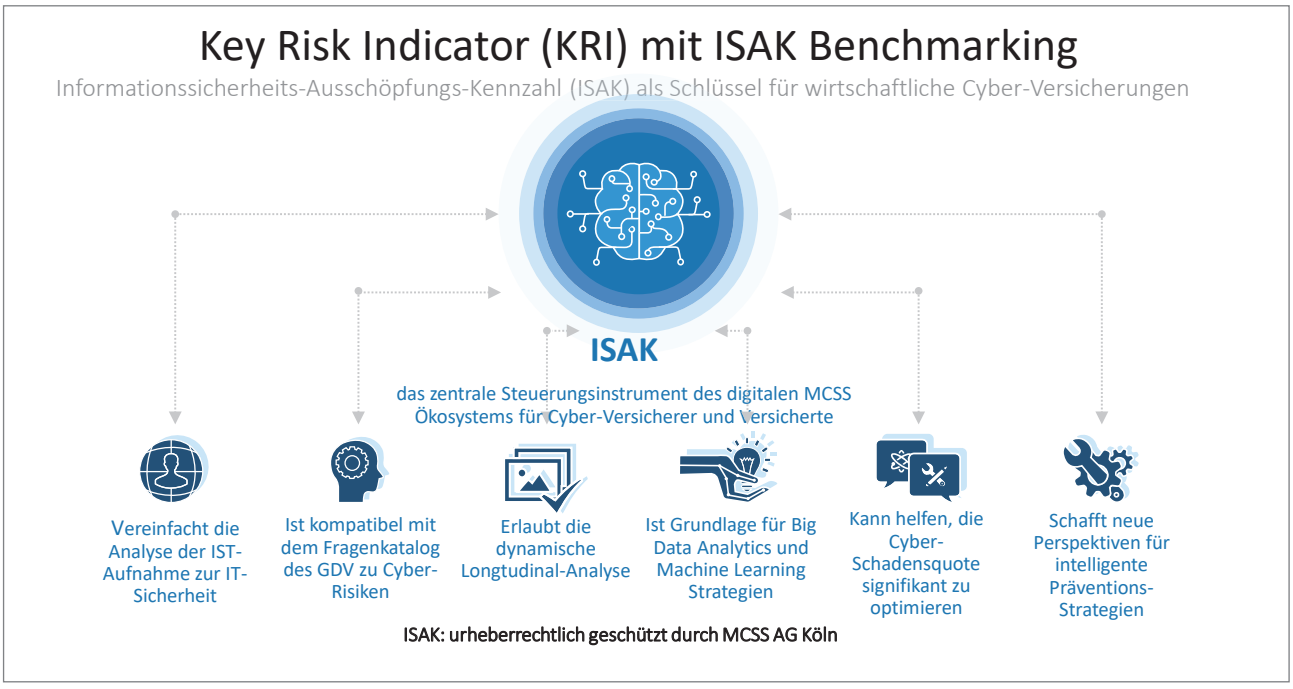
4 Informationssicherheits-Ausschöpfungskennzahl (ISAK)

Das **ISAK** Modell (geschützte Wortmarke der MCSS AG, Köln) wurde ab 2005 von den MCSS Gründungsaktionären im Gesundheitswesen entwickelt. Am Anfang stand die PSAK (Patientensicherheits-Ausschöpfungskennzahl) in der medizinischen Versorgung.

Die Entwicklung der Ausschöpfungs-Kennzahlen (AK) erfolgt nach den Prozessen der strukturierten KRI- und KPI Entwicklung nach internationalen Standards.

Das ISAK Modell wurde nach Qualitätsmanagement-Normen in folgenden Schritten entwickelt:

- Festlegung der Ziel- und Anwendungsgruppen (z.B. Arztpraxen, Krankenhäuser, KMU etc.)
- Definition der relevanten Arbeitsbereiche wie Informationssicherheit (IS) Datenschutz (DS), Qualitätsmanagement (QM)
- Identifikation vorhandener Standard-Strukturen (z.B. Fragenkatalog des GDV zur Cybersicherheit)
- Definition der Datenpunkte und ihre Klassifizierung (z.B. mit 6 Werten in der Bandbreite von „nicht erfüllt“ bis „vollständig erfüllt“
- Auswahl der Fragen/Datenpunkte je nach Anwendung (z.B. zur Einordnung der Obliegenheiten vor Abschluss einer neuen Versicherung (6, 12, 24 Fragen)
- Auswahl der Fragen/Datenpunkte je nach Anwendung (z.B. zur Einordnung der Obliegenheiten während der Vertragslaufzeit (6, 12, 24 Fragen)
- Gewichtung der einzelnen Datenpunkte (Fragen) im Gesamtkontext nach den potenziellen Auswirkungen (Anteil der erreichbaren Punkte zur Gesamtpunktzahl)
- Ermittlung des jeweiligen Algorithmus zur Gesamtgewichtung einzelner Risiko-Komplexe. Dabei wird auf Erfahrungswerte aus QM- und Sicherheits-Projekten im Gesundheitswesen referenziert
- In zukünftigen Forschungsprojekten sollen auf der Grundlage von „Supervised Machine Learning“ Modellen eine branchenübergreifende Verfeinerung der Algorithmen erfolgen (siehe Förderprojekte des BMWi)



Quelle: MCSS AG, Köln. Übersicht zur ISAK, copyright geschützt.

4.1 Datapoints nach GDV Fragenkatalog für Cyber-Versicherer

Der GDV hat bereits im Dezember 2019 einen strukturierten Fragebogen für Risiko-Kriterien für Cyber-Sicherheit herausgegeben:

Der GDV-Fragebogen unterscheidet bereits nach einzelnen Branchen wie:

- E-Commerce
- Dienstleistungen
- Vernetzte Produktion

Weitere Branchen-Ergänzungen können von Versicherern und Assistance Dienstleistern entwickelt werden (siehe MCSS AG in den Branchen Gesundheit und Soziales.

Im Dokument heißt es zum Einsatzzweck:

> *„Der vorliegende Muster-Fragebogen soll es einem Erstversicherer ermöglichen, das Risiko- und Schadenspotenzial eines Versicherungsnehmers mit wenigen Fragen grob, aber aussagekräftig zu erfassen.“*

Tabelle 2. Verteilung der Fragen auf Themenbereiche und Risiko-Kategorien.

		A	B	C	Dienst-leister	Private Geräte	E-Com-merce	Sensible Daten	ICS	Σ
OBLIEGENHEIT	Zugang / Zugriff	4	3						3	10
	Schutz vor Schadsoftware	1								1
	Patching Sicherheits-updates	1	1						1	3
	Backup Datensicherung	4							2	6
	Organisatorische Sicherheit		3	2					2	7
	Netzwerk-separation		1			1			3	5
	Schutz sensibler Daten			1		1				2
	Risikoeinstufung			1	5		3	3		12
	Σ	10	8	4	5	2	3	3	11	

Quelle: „Unverbindlicher Muster-Fragebogen zur Risikoerfassung im Rahmen von Cyber-Versicherungen für kleine und mittelständische Unternehmen“ herausgegeben vom GDV (Dezember 2019)

Beispiel einer Fragestellung aus dem GDV Fragebogen:

> A5. Wöchentliche Datensicherung
>
> **Obliegenheit:** Datensicherung
>
> **Relevanz:** Ohne Datensicherung ist eine Wiederherstellung der Betriebsbereitschaft nur schwer möglich, was eine mögliche Betriebsunterbrechung in die Länge zieht. Ein nachhaltiger Datenverlust kann hohe, teils unwiderrufliche Schäden zur Folge haben.
>
> **Standard-Formulierung:** *Wir schützen uns vor dem Verlust der wichtigsten Unternehmensdaten durch eine mindestens wöchentliche Datensicherung.*
>
> **Vereinfachte Formulierung:** *Machen Sie mindestens einmal pro Woche eine Sicherungskopie Ihrer Daten?*

Da Interessierte für Cyber-Versicherungen sehr „aufwandsensibel“ sind, muss auf einfache Ermittlung der Indikatoren geachtet werden. Der GDV Fragenkatalog bietet deshalb standardisierte und vereinfachte Antwortformulierungen an.

4.2 ISAK im Gesundheitswesen und in der Sozialwirtschaft

ISAK ist ein von der **MCSS AG, Köln**, entwickeltes Analyse- und Bewertungssystem zur Klassifizierung von Cyberrisiken in kleinen und mittleren Unternehmen (KMU), insbesondere im Gesundheitswesen und in der Sozialwirtschaft.

ISAK wird digital mit cloudbasierten IT-Anwendungen ermittelt.
Das System dient der Risikobewertung und dem Monitoring für Cyberversicherungen.

Die jeweilige **ISAK** wird durch die Bewertung von bis zu 120 Datenpunkten innerhalb eines digitalen Ökosystems automatisch berechnet. Der Wertebereich von **ISAK** liegt zwischen 0,60 und 1,20 (1,20 = 20% sicherer als der erreichbare Normal-Standard).
In der Realität liegen die Werte zwischen 0,70 und 1,10.

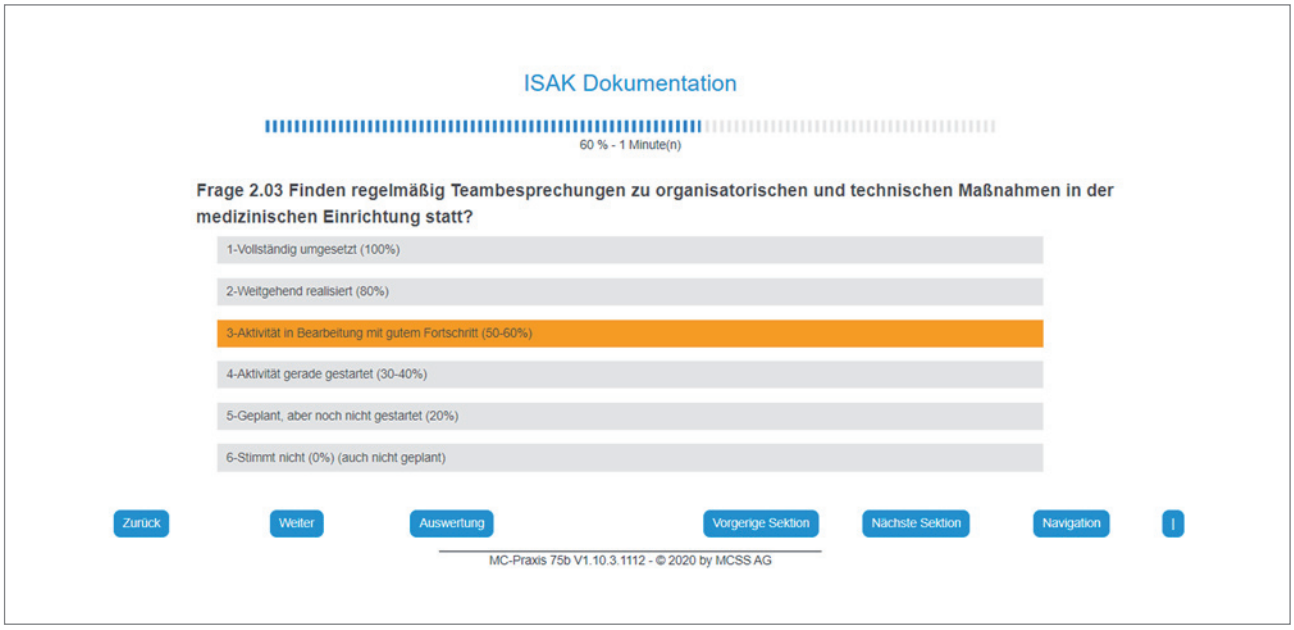
Der Wert 0,7 sagt aus, dass die IT-Sicherheitsmaßnahmen der Organisation nur zu 70% ausgeschöpft werden und somit ein hohes Risiko für Schäden durch Cyberstörfälle besteht.
Der Wert 1,20 sagt aus, dass die technischen und organisatorische Voraussetzungen und Maßnahmen um 20% über dem Sicherheits-Durchschnitt liegen.

Die Algorithmen zur Berechnung und Klassifizierung der **ISAK**-Werte basieren auf langjährigen Beobachtungen und Studien von digitalen Qualitäts- und Sicherheitsmanagementprojekten der MCSS Gründer.

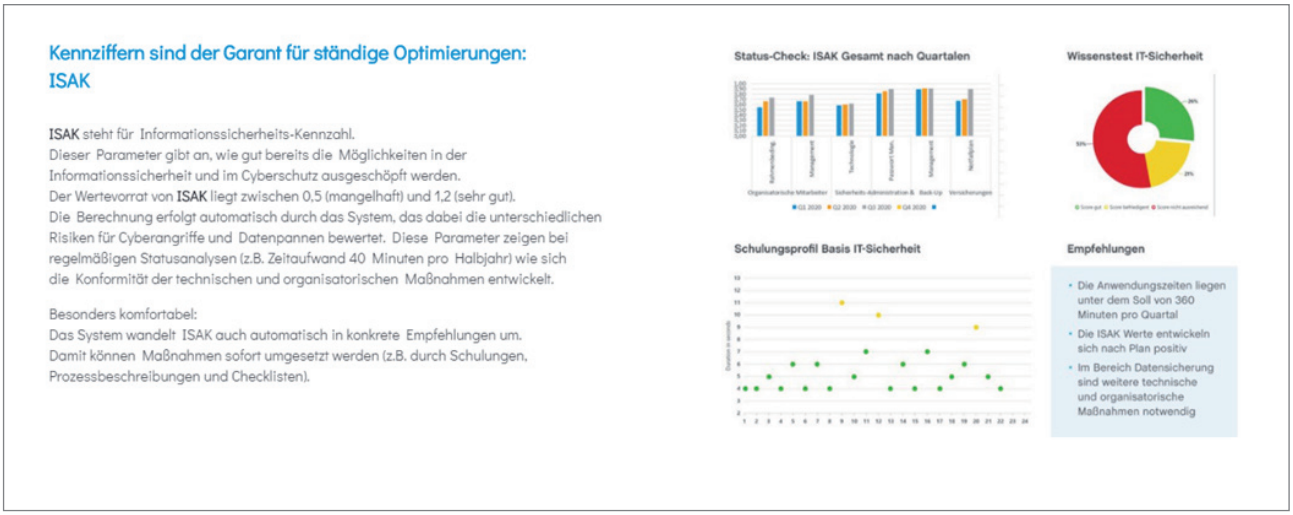
Die globale **ISAK** Auswertung kombiniert verschiedene Bewertungsparameter wie Ergebnisse der Wissenstests, die Nutzung der Schulungskomponenten und die Status-Checks der TOM. Die Empfehlungen sind ein Extrakt der Einzelergebnisse und können direkt von den Verantwortlichen mit zusätzlichen Schulungen (Videos), Verfahrensanweisungen und Maßnahmen angewendet werden.

Spezifische Cyber- und IT-Sicherheitsrisiken in der ambulanten medizinischen Versorgung	Gesamtrisiko von 100%	Nutzeranteil (Schätzung Mai 2021)	Richtlinien (KBV) und Referenzen
Anwendungen in der Arztpraxis			
Telematikinfrastruktur (TI) (z.B. eAU etc.)	**10,5%**	**95,0%**	§ 75b Anl. 5 Ziffer 1–7
Medizintechnik Datenschnittstellen (HL7, DICOM, GDT)	**10,0%**	**60,0%**	§ 75b Anl. 4 Ziffer 1–6
Qualitätssicherungsprogramme, DMP etc.	**7,5%**	**25,0%**	QM RL § 135ff SGB V / DVG
Webbasierte Terminkalender	**8,5%**	**35,0%**	§ 75b Anl. 1 Ziffer 7–11
Videosprechstunden	**6,5%**	**45,0%**	§ 75b Anl. 1 Ziffer 7–11
eRezept (ab 07/2021)	**8,5%**	**85,0%**	§ 75b Anl. 5 Ziffer 1–2
eArztbrief (KIM)	**6,0%**	**60,0%**	§ 75b Anl. 5 Ziffer 1–2
ePA (Elektronische Patientenakte) (ab 2022)	**9,5%**	**55,0%**	§ 75b Anl. 1 Ziffer 7–11
Forschungsprojekte	**4,5%**	**15,0%**	QM RL § 135ff SGB V / DVG
Gesundheits-Apps	**6,5%**	**10,0%**	§ 75b Anl. 1 Ziffer 7–11
IT-Crashes (technische Störfälle)	**3,5%**		BSI Grundschutz
Cyber-Attacken global	**2,5%**		BSI Grundschutz
Phishing Attacken	**2,5%**		BSI Grundschutz
Sabotage intern	**1,5%**		BSI Grundschutz
Andere Risiken	**12,0%**		BSI allgemein
GESAMT	**100%**		

Quelle: MCSS AG, Köln. Eigene Untersuchungen zur Risikoschätzung zur Anwendung im Rahmen der Digitalisierung im Gesundheitswesen, insbesondere Digitale-Versorgung-Gesetz (DVG).



Quelle: MCSS AG, Köln. Die Fragen werden online im cloudbasierten MCSS System beantwortet. Dazu stehen jeweils sechs Antwort-Alternativen zur Auswahl. Die Anzahl der Fragen und die Spezifizierung richten sich nach der Größe der Einrichtung und der Branche.



Quelle: MCSS AG, **Köln**. Je nach Modul des digitalen MCSS Ökosystems werden auch automatisierte Antworten und Empfehlungen für notwendige technische und organisatorische Maßnahmen angeboten. Der Status-Check zeigt den Reifegrad der Organisation in einzelnen Bereichen an. Die sogenannte „Donut-Grafik" rechts oben zeigt das Ergebnis des Wissenstest der Mitarbeitenden. Das Schulungsprofil zeigt die Anwendung der Schulungsunterlagen an.

4.3 ISAK in kleinen und mittleren Unternehmen (KMU)

Auch in kleinen und mittleren Unternehmen (KMU) werden **ISAK**-Modelle eingesetzt.
Die Bewertungsbereiche können von dem Fragenkatalog des GDV abgeleitet werden.

Die Unterscheidung der Risiko-Kategorien macht deutlich, dass im Cyberschutz das Prinzip „one fits all" (ein einziges System ohne Berücksichtigung der individuellen Branchenanforderungen) zu falschen Ergebnissen bei der Risikobewertung führen kann. Die Risiken unterscheiden sich nach Größenordnungen der Organisationen und den Branchen.

Im GDV Fragenkatalog werden exemplarisch unterschieden nach Unternehmen/Branchen mit:

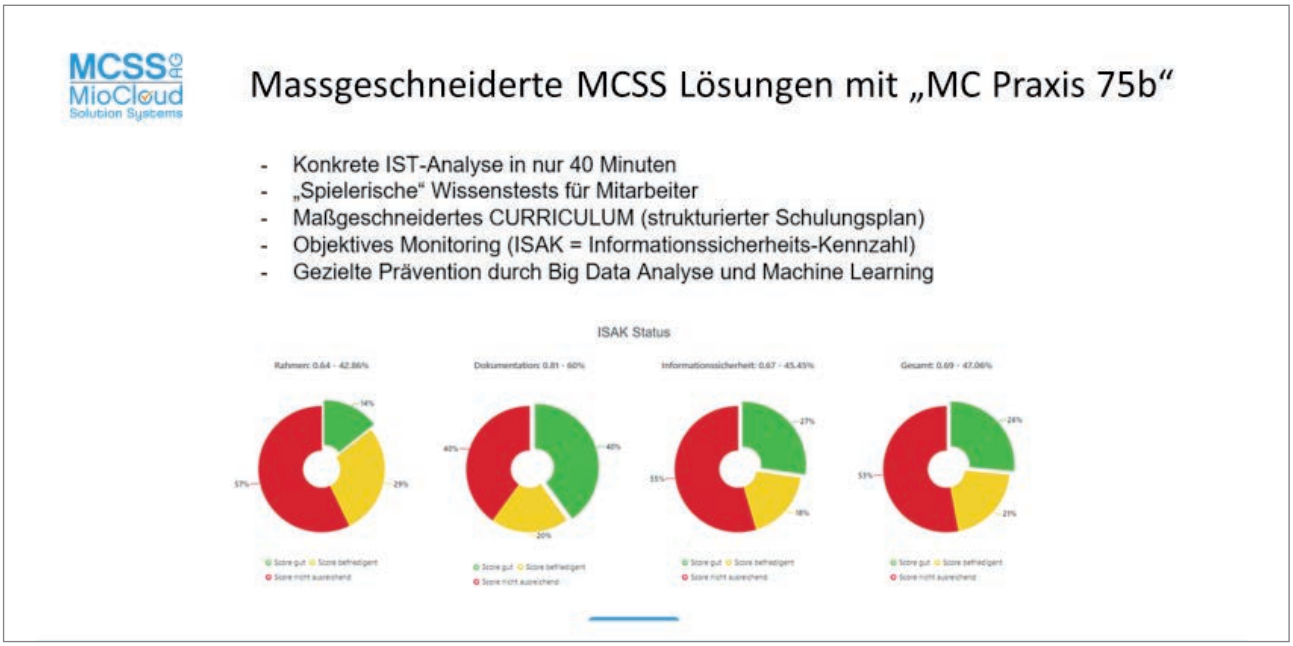
- E-Commerce (mit eigener Infrastruktur)
- Industrial Control Systems (ICS)

Tabelle 1. Kriterien der Risiko-Kategorien A-C.

Risiko-Kategorie	Kriterien
A	▪ Jahresumsatz <= 2 Mio. EUR ▪ *Keiner* der folgenden Geschäftsbereiche: ○ e-Commerce mit eigener Infrastruktur ○ Verarbeitung sensibler Daten, insb. personenbezogene Daten Dritter ○ Berufsgeheimnisse ○ Betriebsgeheimnisse Dritter ○ Industrial Control Systems (ICS)
B	▪ Jahresumsatz <= 5 Mio. EUR ▪ *Max. einer* der folgenden Geschäftsbereiche ○ e-Commerce mit eigener Infrastruktur ○ Verarbeitung sensibler Daten, insb.: besondere personenbezogene Daten Dritter ○ Berufsgeheimnisse ○ Betriebsgeheimnisse Dritter ○ Industrial Control Systems (ICS)
C	▪ Jahresumsatz <= 10 Mio. EUR

Quelle: GDV (Fragebogen zu Cyber-Versicherungen). Der Fragebogen enthält ca. 50 Fragen für die einzelnen Versichertengruppen, die von den Cyber-Versicherern im Rahmen der Vereinbarung von Obliegenheiten eingesetzt werden.

Von der **MCSS AG** wurden KMU Versionen in dem digitalen Ökosystem entwickelt:



Quelle: MCSS AG, **Köln. ISAK** Report Auswertung aus dem digitalen Ökosystem, Version **MC-PRAXIS 75b** (Beispieldaten): Rahmenbedingungen, Dokumentation, Informationssicherheit und Gesamt KRI.

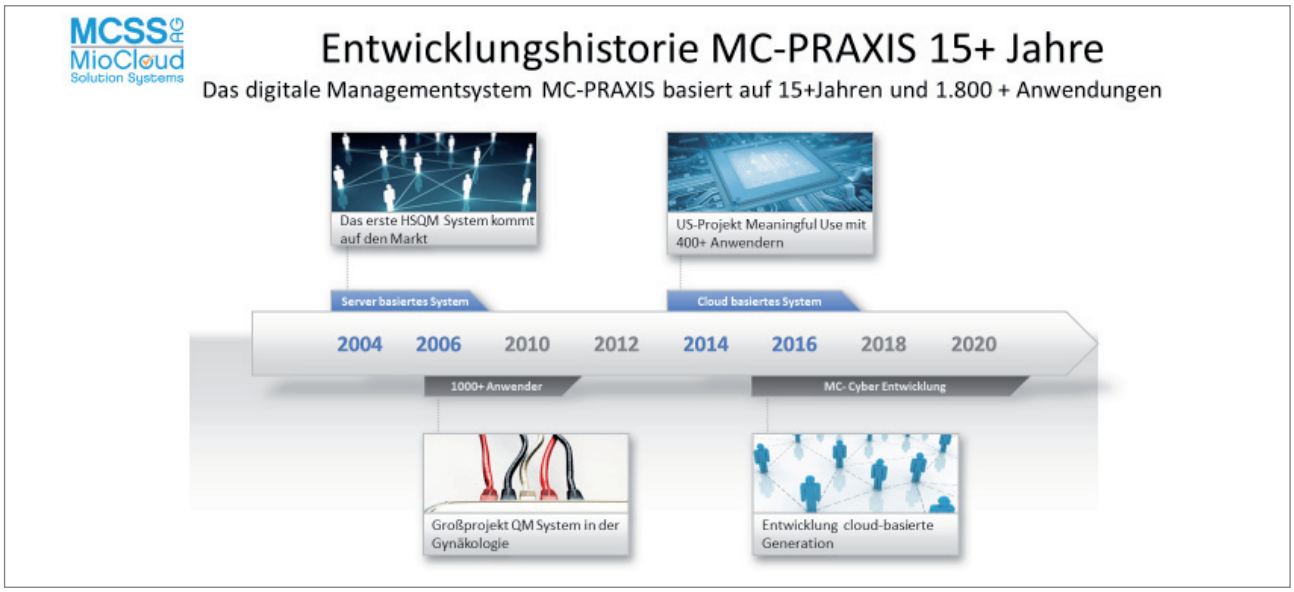
Die **ISAK** Algorithmen lassen sich auf alle Bereiche der KMU-Welt umsetzen: Handel, Handwerker, Gast- und Tourismusbranche, kleine Produktionsbetriebe sowie Selbstständige.

Spezielle **ISAK** Profile wurden für Arzt- und Zahnarztpraxen, Krankenhäuser und Kliniken, Pflegeeinrichtungen, Einrichtungen der Kinder- und Jugendbetreuung sowie kirchliche Einrichtungen entwickelt.

4.4 Historie und Zukunft der ISAK

4.4.1 Historie der Entwicklung

Die Ausschöpfungskennzahlen wie **PSAK** (Patientensicherheit-Ausschöpfungskennzahlen) und **ISAK** (Informationssicherheit-Ausschöpfungskennzahlen) gehen auf Entwicklungen eines QM- und Sicherheitsmanagementsystem in der ambulanten medizinischen Versorgung zurück.



Quelle: MCSS AG, Köln. Das erste digitale System für Sicherheitsmanagement mit einem KRI Modell wurde 2005 durch die MCSS Gründungsaktionäre entwickelt und 2006/2007 in den Markt der medizinischen Versorgung in Deutschland und 2013 in den USA eingeführt.

4.4.2 Forschungsprojekte

Zunehmend nutzen Cyberkriminelle große Rechnerleistungen für Machine Learning und KI-Ansätze für ihre Störattacken. Um auf diesem Niveau mithalten zu können, müssen auch Verteidigungsstrategien innovative IT-Strategien nutzen.

Diese Ansätze setzen strukturierte und vergleichbare Daten voraus. Key Risk Indicators (KRIs) und Key Performance Indicators (KPIs) eignen sich besonders für digitale Evaluierungen von Risiken und den geeigneten technischen und organisatorischen Maßnahmen (TOM).

Das digitale **MCSS Ökosystem** für Informationssicherheit, Cyberschutz und Datenschutz nutzt Machine Learning Konzepte in Forschungsprojekten, die vom Bundesministerium für Wirtschaft (BMWi) gefördert werden.

Quelle: MCSS AG, **Köln.** Entwicklungsabteilung - Informationen zum Forschungs- und Förderprojekt des Bundesministeriums für Wirtschaft und Energie (BMWi) zum IT-basierten Prozessmanagement in der Informationssicherheit (IS), dem Datenschutz (DS) und dem Qualitätsmanagement (QM).

4.5 Beispiele zur Nutzung von Benchmarks im Informationssicherheits- und Datenschutzmanagement

Die großen Vorteile der regelmäßigen Nutzung von Benchmarks zur Erhöhung des Cyberschutzes, der Informationssicherheit und des Datenschutzes werden bei Analyse der Risikopotenziale deutlich.

Diese Auslöser sind:

- Änderungen in der IT-Infrastruktur durch neue oder zusätzliche Hardware und Software (z.B. Wechsel von einer SW-Generation auf die Nächste)
- Veränderungen im Personalbereich (z.B. Austausch des Beauftragten für IT-Sicherheit (ISB))
- Erweiterung oder Verkleinerung der Organisationseinheit mit Einfluss auf die IT-Infrastruktur
- Neue Rechtsnormen für IT-Sicherheit und Datenschutz und damit Risiken von Rechtsfolgen (DSGVO/BDSG und im Gesundheitsbereich § 75b/§ 75c SGB V)

Fälle aus dem Gesundheitsbereich

- Ein Krankenhaus eröffnet eine Außenstelle zur Durchführung von Untersuchungen (Diagnose-Zentrum). Dazu werden Verbindungen zwischen dem primären Standort und dem externen Diagnose-Zentrum hergestellt. Das Risiko für Sicherheitsvorfälle steigt erheblich, was an einem niedrigeren **ISAK** abgelesen werden kann (Beispiel: **ISAK** sinkt von 0,85 auf 0,75). Der ISB und der Cyber-Versicherer müssen reagieren.
- In einem Krankenhaus verlässt der IT-Leiter das Unternehmen und ein Nachfolger kann erst 3 Monate später eingesetzt werden. Dadurch geht umfangreiches Wissen zur IT-Sicherheit verloren und die Risken für Störfälle steigen erheblich. Mit regelmäßigen **ISAK**-Erfassungen werden die Lücken transparent und die Verantwortlichen können gegensteuern (organisatorische Maßnahmen)
- Ein ophthalmologisches ambulantes OP-Zentrum übernimmt eine traditionelle Augenarztpraxis. Die Diagnosedaten der Patienten müssen digital zwischen heterogenen Praxisverwaltungssystemen (PVS) übertragen werden. Das Risiko für unerwartete Störfälle steigt erheblich. Dies kann in regelmäßigen oder anlassbezogenen **ISAK**-Prüfungen sofort visualisiert werden (**ISAK** sinkt von 0,88 auf 0,72)
- Ein Krankenhaus installiert ein neues medizinisches Großgerät, das mit einem PACS (Picture Archive and Communication System) verbunden wird und mit einer DICOM-Systemlösung installiert wird. Das Risiko für digitale Störungen kann erheblich steigen. Dies kann durch die **ISAK**-Bewertung transparent gemacht werden.
- Aus einer Einzelpraxis wird eine größere Gemeinschaftspraxis unterschiedlicher Facharztbereiche. Die verschiedenen Diagnosegeräte müssen im lokalen Netzwerk verbunden werden. Das technische „Change-Management“ kann neue und zusätzliche Risiken für die Informationssicherheit (und den Datenschutz) bedeuten. Weigehend objektiv können diese Risiken nur durch Benchmarks (KRIs) transparent gemacht werden.
- Der Leiter einer zahnmedizinischen Klinik war nicht über die gesetzlichen Rahmenbedingungen mit Einführung der IT-Sicherheitsrichtlinie nach § 75b informiert. Erst eine Statusanalyse mit KRI machte deutlich, dass Lücken in der Rechtskonformität vorhanden waren, da der **ISAK** Parameter eine deutlich negative Bewertung der Risikoeinstufung auswies.

5 Handlungsempfehlungen

Bislang ist die Vorbereitung auf Cyberattacken und IT-Störfälle in fast allen Anwendungsbereichen lückenhaft und unvollständig. Um die begrenzten finanziellen und zeitlichen Ressourcen nach Prioritäten optimal einzusetzen, ist der Einsatz objektiver Risiko-Indikatoren unabdingbar. Parallel dazu sind auf die Risiken abgestimmte Cyber-, Betriebsunterbrechungs- und Haftpflicht-Versicherungen dringend angeraten.

Viele Versicherer bieten inzwischen zur Unterstützung ihren Kunden sogenannte Assistance Dienstleistungen an. Versicherte sollten darauf achten, dass die wichtigen Unterstützungskonzepte auf innovativen und transparenten KRI basieren.

Diese speziellen Benchmarks machen die Zusammenarbeit mit IT-Anwendern, ihren Dienstleistern und Versicherern transparent. Diese Transparenz fördert ein ausgewogenes Konditionsmanagement und gegenseitige Fairness im Falle einer Schadensregulierung.

6 Zusammenfassung

Die fortschreitende Digitalisierung in vielen Bereichen erhöht die Produktivität und Effizienz vieler Prozesse z.B. in der Wirtschaft, dem Handel sowie im Gesundheitswesen und der Sozialwirtschaft. Damit verbunden sind explodierende Datenmengen und leider auch steigende Risiken für die Informationssicherheit und den Datenschutz. Die Digitalisierung fördert auch den Einsatz innovativer digitaler Instrumente. In den unterschiedlichen Branchen werden zunehmend strukturierte Datenformate entwickelt und veröffentlicht:

- Das BSI veröffentlicht Kriterien, die in Benchmark-Konzepten umgesetzt werden können. Beispiel: HV-Benchmark (Hochverfügbarkeits-Benchmark für professionelle IT-Umgebungen)
- Der Verband der deutschen Versicherer (GDV) hat einen Fragekatalog entwickelt, der für ein Benchmarking relevante Fragen zur Informationssicherheit im Rahmen von Cyber-Versicherungen zur Verfügung stellt.
- Das Gesundheitsministerium hat mit dem Projekt „Digital Radar“ die digitale Reifegradmessung im Gesundheitswesen eingeführt.
- Die Kassenärztliche Bundesvereinigung (KBV) hat in Zusammenarbeit mit der Bundesärztekammer und mit Koordination des BSI die Kriterienliste nach § 75b SGB V im Dezember 2020 veröffentlicht.
- Von der MCSS AG, Köln, wurde auf der Grundlage einer mehr als 15-jährigen Erfahrung mit KRIs und KPIs das Modell der **ISAK** entwickelt.
- Mit den **ISAK** Parametern lassen sich gezielt die Maßnahmen im Sicherheits- und Qualitätsmanagement umsetzen und für die Mitarbeitenden transparent im Coaching umsetzen.
- Kontinuierliche Verbesserungen nach der PDCA (Plan-Do-Check-Act) Strategie lassen sich mit objektiven KRIs wie **ISAK** im modernen Team-Coaching fair realisieren.

Der wesentliche Vorteil von KRIs und KPIs ist die Nutzung der Benchmark-Daten für innovative IT-Anwendungen wie Big Data Analysen und Machine Learning bis hin zur Künstlichen Intelligenz (KI). Erst durch strukturierte Datenmodelle lassen sich die Potenziale der IT 4.0 wirklich effektiv nutzen.

7 Die Autoren

Stephan Engels

Stephan Engels ist Vorstandsvorsitzender der **MCSS AG** (MioCloud Solution Systems) in Köln.
Er ist Diplom-Betriebswirt (MBA) und zertifizierter Datenschutzbeauftragter und betreut in dieser Funktion viele Arztpraxen in Deutschland.

In eigenen Vor-Gesellschaften hat Stephan Engels mehr als 30 Jahre Erfahrung im Bereich Health-IT und Web-Marketing für Arztpraxen gesammelt.

Mit einem spezialisierten Team hat er neue und innovative Datenmanagementsysteme für Qualitätsmanagement (QMS) und Datenschutz (DSMS) für Arztpraxen entwickelt.

Es ist ihm ein besonderes Anliegen, Ärzte(innen) bei der Überwindung der Bürokratie zu unterstützen und dabei neue Wege mit IT-Lösungen zu gehen.

Christian Schottmüller

Christian Schottmüller studierte Betriebswirtschaftslehre und Jura an der Universität in Köln.

Seit dem Jahr 2008 ist er in verschiedenen Leitungsfunktionen für die Versicherungswirtschaft tätig und arbeitete dort seit 2014 unter anderem daran mit, Standards für die IT-Sicherheit im präventiven Bereich durch Informationssicherheits-Managementsysteme zu entwickeln. In seiner Laufbahn vermittelte er sein profundes Branchenwissen in zahlreichen Schulungen und Vorträgen.

Im Jahr 2021 übernahm Christian Schottmüller die Verantwortung für die Umsetzung von Cyberschutz und Informationssicherheit im Gesundheitswesen und in der Sozialwirtschaft als Direktor der **MCSS AG, Köln**.

Rainer Waedlich

Rainer Waedlich ist Experte für Health-IT (E-Health), Cyberschutz und Qualitätsmanagement im Gesundheitsbereich. In seiner über 40-jährigen Berufslaufbahn im Gesundheitswesen hat er – national und international – softwarebasierte Produkte im Bereich der elektronischen Patientenakte (EPA), Qualitätssicherung und Qualitätsmanagement entwickelt und über 1.000 Arztpraxen und Kliniken weltweit in IT-Fragen beraten.

Im Bereich Big Data Analytics und Machine Learning hat Rainer Waedlich in internationalen Projektgruppen an Health-IT Anwendungen, u.a. mit IBM Watson Teams in den USA und Japan gearbeitet.

Als Aufsichtsratsvorsitzender deutscher und amerikanischer Health IT-Unternehmen war er 15 Jahre lang u.a. für die Rechtskonformität von wissensbasierten Projekten verantwortlich (Entwicklung von Algorithmen für Vorstufen von KI-Anwendungen, „Artificial Intelligence in Medicine“).

Sein Spezialgebiet, neben E-Health, sind Optimierungs-Strategien im organisatorischen und versorgungstechnischen Bereich, z.B. mit KAIZEN Konzepten (KAIZEN = das japanische Prinzip der ständigen Optimierung).
Aktuell ist er Aufsichtsratsvorsitzender der **MCSS AG, Köln** und im Unternehmen verantwortlich für Rechtskonformität von IT-Anwendungen.

8 Referenzen/Anlagen

- Unverbindliche Bekanntgabe des Gesamtverbandes der Deutschen Versicherungswirtschaft e.V. (GDV) zur fakultativen Verwendung: Muster-Fragebogen zur Risikoerfassung im Rahmen von Cyber-Versicherungen
- Veröffentlichungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu Umfragen zur Cybersicherheit
- Veröffentlichung der Academy of Health Information Management Executives (AHIME) (Digital Health Most Wired Survey) zum digitalen Reifegrad-Modell für Krankenhäuser

Anmerkung

Das digitale **MCSS Ökosystem** wurde vom Bundesministerium für Wirtschaft (BMWi) im Rahmen eines ZIM Forschungs- und Innovationsprojekts gefördert.

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

ZIM
Zentrales
Innovationsprogramm
Mittelstand

MCSS AG
MioCloud
Solution Systems

A Weinsbergstraße 190
50825 Köln
T 0221/47 44 77 44
F 0221/47 44 77 55
E info@mcss-ag.de
W mcss-ag.de