Heft 40 | Dezember 2024 | 18. Jahrgang | ISSN 1864-6557

IT-GOVERNANCE

Fachzeitschrift des ISACA Germany Chapter e.V.

IT-Prüfung

Prüfkatalog für das neue IT-Audit-Thema »Gesetzeskonformer Umgang mit IT-Diagnose-Daten«

Stephen Fedtke

Sonderdruck

ISACA Germany Chapter

dpunkt.verlag | it-governance.dpunkt.de | isaca.de

Sonderdruck
aus:

IT-Governance
Fachzeitschrift des ISACA Germany Chapter e.V.

http://it-governance.dpunkt.de/

18. Jahrgang – Heft 40 – Dezember 2024
Seiten 29–36

ISSN 1864-6557

IT-Prüfung

Prüfkatalog für das neue IT-Audit-Thema »Gesetzeskonformer Umgang mit IT-Diagnose-Daten«

Stephen Fedtke

IT-Diagnose-Daten lenken den Fokus auf ein neues IT-Audit-Thema: die sensiblen Daten in Dumps, Logs und Traces. Sie enthalten IT-Sicherheitsinformationen und gleichzeitig datenschutzrelevante Daten mit Personenbezug. Geraten diese unerlaubterweise und zweckfrei an Dritte, verletzt der Versender Gesetze sowie Normen und Rahmenwerke wie die europäische Datenschutz-Grundverordnung (DSGVO), das Schweizer Bundesgesetz über den Datenschutz (DSG), die Network-and-Information-Security-Richtlinie 2.0 (NIS-2), den Digital Operational Resilience Act (DORA) oder den Payment Card Industry Data Security Standard (PCI-DSS). Für Institutionen kritischer Infrastrukturen (KRITIS), wie u. a. dem Gesundheitswesen, ist das Monitoring dieser potenziellen Datenlecks von besonderer Relevanz.

Der aktuelle Trend auf Basis der Rechtsprechung des EuGH zum immateriellen Schadensersatzanspruch im Sinne des Art. 82 DSGVO geht in Richtung Massenklagen und Beweislastumkehr. Daneben steht die Rechtsentwicklung um Security-bezogene Pflichten, wie NIS-2, DORA, PCI-DSS. Dies führt bei Unternehmen und deren Leitungsebene zu erhöhten Obliegenheiten und Haftungsrisiken. Aus diesem Grund sind IT-Diagnose-Daten künftig ein sehr wichtiges Prüffeld des IT-Audits und der IT-Revision, unabhängig davon, ob die IT-Systeme intern oder extern betrieben werden.

1 Detaillierte Prüfkataloge »IT-Diagnose-Daten«

Die nachfolgenden Prüfkataloge beinhalten implizit einen Prüfplan. Sie ermöglichen eine umfängliche, konkrete und detaillierte Prüfung des IT-Betriebs auf rechtskonformen und sicheren Umgang mit IT-Diagnose-Daten. Neben der Option zur grundsätzlichen Vermeidung von IT-Diagnose-Daten besteht die rechtskonforme Maßnahme in der Bereinigung der sensiblen Daten vor dem Upload. Eine solche Anonymisierung ist als Prüfpunkt in den Katalogen enthalten.

Der Katalog repräsentiert zudem einen möglichen Ablaufplan der Prüfung:

1. **Prüfkatalog** »**G**« konzentriert sich auf »grundsätzliche Prüfungen«, d. h. auf das Vorhandensein klarer innerbetrieblicher Regelungen und einer soliden Awareness zum Thema IT-Diagnose-Daten.
2. **Prüfkatalog** »**I**« konzentriert sich auf die »Inhouse-Handhabung« von IT-Diagnose-Daten, wie im Falle einer eigenen Softwareentwicklung.
3. **Prüfkatalog** »**K**« konzentriert sich auf die »transparente Kommunikation der Bereinigung gegenüber relevanten Parteien«, d. h. auf notwendige und sinnvolle Kommunikationen über a) die Risiken von IT-Diagnose-Daten im Sinne der Awareness, b) die Notwendigkeit der Bereinigung und c) die proaktive Offenlegung der Tatsache angewandter Bereinigungen, z. B. gegenüber den Softwareherstellern.
4. **Prüfkatalog** »**E**« ist optional, denn er konzentriert sich auf »IT-Diagnose-Daten im Falle der Inanspruchnahme von Serviceprovidern«, d. h. auf deren Verpflichtung und eine Anleitung zur Zusammenarbeit.
5. Die Anleitung zur **stichprobenbasierten Überprüfung** bildet den Übergang von der »Paper-based Compliance«, basierend auf Dokumentenprüfung, zu der Realität des IT-Alltags. Eine solche Prüfung beinhaltet die Auditierung des IT-Betriebs und eine Auswahl bereits erfolgter Uploads von IT-Diagnose-Daten und deren konformer Handhabung.

Jeder einzelne Prüfpunkt eines Prüfkatalogs verfügt über eine eindeutige ID, mit der Querreferenzen einfach möglich sind. Außerdem enthält er das Prüfthema und eine beispielhafte Ausprägung.

2 Prüfkatalog »G«: Grundsätzliche Prüfthemen

Die Fragen decken das Fundament eines sicheren, risikominimalen und rechtskonformen Umgangs mit IT-Diagnose-Daten ab.

ID	Prüfthema	Ausprägung
G.01	Gibt es im IT-Betrieb eine dokumentierte Verfahrensvorgabe für den Umgang mit IT-Diagnose-Daten? Hinweis: • Bezüglich notwendiger Awareness siehe auch K.01.	• Existiert eine eigenständige Dokumentation, z. B. ein Kapitel bzw. ein Abschnitt im Betriebshandbuch verbunden mit klaren Handlungsanweisungen? • Existiert eine klare Definition des Begriffs »IT-Diagnose-Daten« (siehe G.02)? • Werden die Verfahrensanweisungen offen kommuniziert? (siehe u. a. K.02) • Gelten aufgrund geschäftlicher Aktivitäten, Kooperationen und Verflechtungen ggf. ergänzende Auflagen, Gesetze und Verordnungen?
G.02	Sind die Begriffe »IT-Diagnose-Dokumente« bzw. »IT-Diagnose-Daten« ausreichend präzise definiert, sodass alle relevanten Dokumentenarten eingeschlossen sind? Hinweis: • Verweis auf G.10: Das Risiko IT-Diagnose-Daten bezieht sich nicht nur auf die DSGVO, sondern auch auf die sicherheitstechnischen Details, die in IT-Diagnose-Dokumenten versteckt eingelagert sind.	• Gibt es präzise Definitionen und Erläuterungen für Dumps, Logs und Traces und deren Varianten? • Sind die Arten und Lokationen für IT-Diagnose-Daten explizit aufgeführt, ohne dass die Auflistung einschränkend wirkt? Zum Beispiel Systeme (Server), Clients, Applikationen, Middleware, Webserver, Appliances, IoT und Mobile Devices. • Ist das Anwendungsgebiet der Regelungen um IT-Diagnose-Daten klar ausgesprochen und definiert, und zwar so, dass sie für alle Betriebssysteme, Systeme, Devices, Plattformen und Appliances, ferner für Test, Entwicklung und Produktion gelten? • Sind eventuelle Abweichungen für Test, Entwicklung und Produktion klar geregelt und abgegrenzt (siehe auch Prüfkatalog »I«)?
G.03	Welche Maßnahmen wurden ergriffen, um das Risiko von IT-Diagnose-Daten zu minimieren bzw. zu eliminieren? Hinweise: • Teilweise bieten Betriebssysteme auch Konfigurationsmöglichkeiten zum Unterdrücken von IT-Diagnose-Daten. • Bezüglich der Anforderung »lokal« siehe G.13. • Bezüglich der Anforderung »Awareness« siehe K.01.	• Stehen entsprechende Tools oder Verfahren zur automatisierten, revisionsgerechten, lokalen Bereinigung von IT-Diagnose-Dateien um sensible Daten bereit? • Sind die betroffenen Parteien über deren Verfügbarkeit im Sinne einer Awareness informiert?
G.04	Sind alle potenziell Beteiligten verpflichtet worden, IT-Diagnose-Daten gemäß den Richtlinien zu handhaben?	• Wurde die Gruppe der zu verpflichtenden Personen in einer Weise definiert, dass alle relevanten Personen, Rollen und Abteilungen sich unmittelbar angesprochen und verpflichtet fühlen (z. B. Administratoren, Datenbankverantwortliche, Entwickler)?
G.05	Ist ebenso die Handhabung im Falle besonders hoher Dringlichkeit geregelt? Zum Beispiel sollte der Zeitbedarf für den Bereinigungsprozess durch eine Fokussierung auf die besonders sensiblen Datentypen reduziert werden. Hinweis: • Gefragt ist die Festlegung einer pragmatischen »Graustufe« zwischen IT-Diagnose-Dokument im Original versenden und die übliche vollständige Bereinigung abwarten.	• Besteht eine Auswahl der essenziell kritischen sensiblen Datentypen, die auch Teil einer eventuellen »Eil-Bereinigung« sein müssen?
G.06	Werden sämtliche Uploads von IT-Diagnose-Daten im Rahmen des Problem-Managements ausreichend dokumentiert und übergreifend aufgezeichnet?	• Besteht für alle betroffenen Parteien die Verpflichtung zum Pflegen entsprechender Aufzeichnungen über den Upload von IT-Diagnose-Daten? • Werden u. a. Datum, Uhrzeit, Bearbeiter, Quellsystem der IT-Diagnose-Daten, Hersteller (Empfänger), Ticketsystem-Name bzw. -URL, Ticket-ID/-Nr. etc. in der Aufzeichnung festgehalten? • Erfolgen diese Aufzeichnungen unabhängig von einer vorangehenden Bereinigung (siehe G.03)? • Gibt es ein eigenverwaltetes zentrales Verzeichnis, in dem alle Akteure sämtliche Uploads dieser Art festhalten, unabhängig von der Methode?
G.07	Haben nur Administratoren Zugriff auf IT-Diagnose-Daten der jeweiligen Systeme?	• Sind sämtliche Zugriffsrechte strikt geregelt? • Sind entsprechende Rollen definiert? • Wird das Entstehen von IT-Diagnose-Daten auf den jeweiligen Systemen automatisch erkannt, festgehalten und ggf. gemeldet (siehe auch G.19)?

→

ID	Prüfthema	Ausprägung
G.08	Erfolgt der Upload, d. h. der Transfer, verschlüsselt? Hinweis: • Alternativ können IT-Diagnose-Daten vor dem Versand in einen verschlüsselten Container verpackt und z. B. als encrypted ZIP-File übertragen werden.	• Ist für Ticketsysteme- oder Upload-Websites der Zugriff über https verpflichtend? • Ist für den Fall eines regulären File-Transfers festgelegt, dass entweder SFTP oder eine andere Methode der verschlüsselten Übertragung verwendet wird? • Sind alle Beteiligten zur Dokumentation sämtlicher Transfer- und Verschlüsselungsdetails (vollständiger Datei- bzw. Pfadname) verpflichtet, unabhängig von Übertragungsmethode oder -werkzeug?
G.09	Sind sämtliche automatischen Transfers von IT-Diagnose-Daten zu Herstellern untersagt bzw. deaktiviert?	• Sind automatische Transfers im Betriebshandbuch und der Security-Policy explizit als »verboten« deklariert worden? • Prüfen und alarmieren vorhandene Policy-Check-Tools entsprechende regelverletzende Systemkonfigurationen automatisch?
G.10	Ist das Spektrum sensibler und damit zu bereinigender Datentypen mit dem Datenschutz-, Risiko- und Sicherheitsmanagement abgeklärt und schriftlich festgelegt worden? Hinweis: • Wichtig ist, dass das Spektrum mindestens die drei Basisdatenkategorien umfasst: a) DSGVO-und DSG-relevante Daten, b) sicherheitssensible Daten und c) individuelle Firmengeheimnisse und Geschäftsdaten.	• Hat die Abteilung Datenschutz dem Spektrum sensibler und damit zu bereinigender Personendaten schriftlich zugestimmt? • Hat das Sicherheits- und Risikomanagement die zu bereinigenden sicherheitssensiblen Daten festgelegt? • Werden erhöhte Auflagen für besonders schützenswerte Daten erfüllt, wie z. B. für mögliche Gesundheitsdaten? • Werden potenziell Gesundheitsdaten verarbeitet (Art. 4 Nr. 15 DSGVO)?
G.11	Was passiert mit den Original-IT-Diagnose-Dateien? Wo werden diese gespeichert? Wann werden diese gelöscht? Wer darf auf die Dateien zugreifen (vgl. CWE[1]-528)?	• Werden gesetzliche oder firmenintern festgelegte Löschfristen eingehalten? • Sind solche Fristen in Abhängigkeit vom Zweck und der Dauer der Analyse festgelegt? • Werden eventuelle Absprachen mit dem Betriebsrat in Bezug auf Logdateien eingehalten?
G.12	Wie sind die Speicherung, Verarbeitung und Löschung aufseiten der Softwarehersteller geregelt? Hinweis: • Wenn nur bereinigte Dokumente übertragen werden, kann die gesamte Situation flexibler gehandhabt werden, weil diese z. B. anonymisierten Dokumente kein DSGVO-Risiko darstellen.	• Sind sämtliche Details durch bestehende Verträge zur Auftragsverarbeitung geregelt? • Oder ist ein Verzicht auf den Empfang von IT-Diagnose-Daten mit dem Hersteller vereinbart? • Ist der Zweck der Übertragung auf die Identifikation und Lösung von Software- und Hardwareproblemen eingegrenzt? • Sind unerwünschte Verarbeitungen, wie z. B. das Trainieren von eigenen Modellen, explizit verboten bzw. geregelt und genehmigt worden?
G.13	Auf welchen Systemen erfolgt die »lokale« Bereinigung? Hinweise: • Würde theoretisch ein externer Service genutzt, z. B. in der Cloud, wäre das gesamte Portfolio an Risiken potenziert, weil sich ein solcher Dienstleister ausschließlich mit den eigenen Geheimnissen beschäftigen würde, um diese zu finden und zu bereinigen. • Das Zugriffsrecht auf eine Bereinigungsumgebung impliziert meist den Zugriff auf aktuell verarbeitete Original-IT-Diagnose-Dokumente anderer Parteien (z. B. Abteilungen) und deren Begleitdaten.	• Erfolgt die Bereinigung auf lokalen, d. h. in keinem Fall auf Systemen Dritter oder im Internet verfügbaren Services? • Auf welchen eigenen Systemen erfolgt die lokale Bereinigung? • Wer hat auf diese lokalen Bereinigungsumgebungen Zugriff?
G.14	Wird die Bereinigung in aussagekräftigen Begleitdokumenten erfasst und nachweisbar festgehalten? Hinweis: • Die Begleitdokumente zu jeder Bereinigung sind als juristischer Entlastungsnachweis essenziell – es ist ein probates Mittel gegen eine Beweislastumkehr.	• Werden mindestens folgende Details als Nachweis festgehalten: Dateinamen, Spektrum gesuchter und gefundener Datentypen, aufgetretene Besonderheiten (Warnings, Errors), explizit »gewhitelistete« Fundstellen bzw. Bereiche und Ergebnisse der Qualitätssicherung (siehe G.21). • Werden im Falle von IT-Diagnose-Daten-Containern (siehe G.16) für alle darin enthaltenen Dokumente gleichfalls diese Auskünfte als Entlastungsnachweis dokumentiert oder zumindest zusammengefasst?
G.15	Welche Arten von Folgeverarbeitungen von IT-Diagnose-Daten werden praktiziert? Hinweis: • Dumps und Traces werden üblicherweise nicht an ein Security Information and Event Management (SIEM) geleitet.	• Werden Log- und Protokolldaten z. B. an/durch SIEM-Lösungen weitergeleitet und verarbeitet? • Wird das SIEM intern oder extern betrieben? • Welche externen Parteien haben auf diese Datensammlungen potenziellen Zugriff, z. B. zwecks forensischer Analysen?

→

1 CWE – Common Weakness Enumeration.

ID	Prüfthema	Ausprägung
G.16	Werden IT-Diagnose-Dokumenten-Container ebenfalls einer Bereinigung unterzogen? Hinweise: • Manche Betriebssysteme erstellen im Problemfall automatisch pax-, tar- oder zip-Files, mit mehreren Hundert oder Tausend Einzeldokumenten. • Diese Container-Files können nicht per se als Einzeldatei bereinigt werden. Stattdessen müssen sie erst entpackt werden. Danach wird jedes einzelne Dokument bereinigt. Am Ende wird dann wieder ein entsprechender Container-File mit den einzelnen bereinigten IT-Diagnose-Dateien erstellt.	• Erfolgt die Bereinigung der enthaltenen IT-Diagnose-Dateien vollständig? • Werden im Falle von Dokumenten-Containern für sämtliche eingebetteten Dokumente ebenfalls entsprechende Begleitdokumente erstellt (siehe G.14)?
G.17	Wie ist der Umgang mit ausführbaren Dateien als Bestandteil von IT-Diagnose-Daten geregelt? Hinweis: • Im Vergleich zu binär codierten Dateien eines unbekannten Formats (siehe G.18) kann hier die As-is-Weitergabe durchaus gerechtfertigt werden. Die Wahrscheinlichkeit, dass diese Executables individuelle sensible Daten beinhalten, ist äußerst gering.	• Werden im Rahmen der Bereinigung ausführbare Dateien (z. B. eine Kopie des sog. Kernels oder exe-, dll- oder ähnliche Dateien) als solche identifiziert und spezifisch gemäß den Richtlinien behandelt?
G.18	Wie ist der Umgang mit binär codierten IT-Diagnose-Dateien geregelt, d. h. mit Dateien, deren binären Inhalte aufgrund fehlenden Wissens über die genauen Formate nicht inspiziert und damit bereinigt werden können? Hinweise: • Eine Weitergabe solcher binär codierten Dokumente impliziert ein Restrisiko, dass diese Binärdaten nicht nachvollziehbare Geheimnisse umfassen könnten, z. B. IP-Adressen. • Dumps sind grundsätzlich ebenfalls binär codiert, sie sind aber so typisch, dass sie von entsprechenden Bereinigungstools unterstützt werden. • Alternative: Vom Hersteller wird das Tool zur »Lesbarmachung« solcher Dateien gefordert. Man erstellt die Reports dann selbst, bereinigt diese und überträgt den bereinigten Report.	• Werden nicht explizit unterstützte binär codierte IT-Diagnose-Dateien vom Upload ausgeschlossen? • Oder werden sie einfach »as-is« weitergereicht? • Stellt der Hersteller ggf. ein Tool zur Lesbarmachung bereit?
G.19	Ist auf den Quellen für IT-Diagnose-Daten, wie z. B. Servern oder Clients, eine Detektion des Entstehens von IT-Diagnose-Dokumenten etabliert? Hinweise: • Erst durch eine solche Aufzeichnung entsteht eine 360-Grad-Vollständigkeit: Sie können a) feststellen, wann und wo welche IT-Diagnose-Daten entstanden sind, b) was mit ihnen passiert ist, c) aus welchen Problemmeldungen gegenüber Herstellern Tickets hervorgegangen sind und d) welche Tickets IT-Diagnose-Daten als Anhang hatten. • Da ein SIEM von Event-Meldungen lebt, müssen entsprechende Sensoren bzw. Agenten die relevanten Ereignisse und Meldungen festhalten und z. B. an das SIEM weiterleiten.	• Stellt das Betriebssystem oder ein Agent die Entstehung von IT-Diagnose-Daten fest? • Wird das Erzeugen von IT-Diagnose-Daten im SIEM oder einem anderen Audit-Log festgehalten?
G.20	Ist ein Remote-Access des Herstellers auf die eigenen Systeme zwecks Vor-Ort-Analysen oder einer Art »Selbstbedienung« vorgesehen? Hinweis: • Bezüglich automatischer Transfers siehe G.09.	• Sind entsprechende Zugriffe nur auf Anfrage oder explizite Freischaltung möglich? • Werden entsprechende Sitzungen aufgezeichnet (Screen-Recording)? • Ist eine Art »Selbstbedienung« ausgeschlossen? Das heißt, werden alle Rücktransfers verboten bzw. überwacht?

→

ID	Prüfthema	Ausprägung
G.21	Existieren Qualitätsanforderungen an die eingesetzte Lösung zur Bereinigung von IT-Diagnose-Dokumenten? Hinweise: • Die Bereinigungslösung muss in mehrerlei Hinsicht eine maximale Qualität anstreben: a) alle relevanten Dokumenten- und Datentypen unterstützen, d. h. kennen und finden, und b) starke Instrumente der Qualitätssicherung anwenden, um sowohl »Leftovers« zu finden als auch den Erhalt des technischen Wertes der bereinigten Dokumente zu verifizieren. • Siehe auch G.14, K.03.	• Werden die bereinigten Dokumente nochmals nach »Leftovers« durchsucht, um eventuell übersehene Daten zu entdecken? • Wird der technische Wert der anonymisierten Dokumente nochmals validiert?
G.22	Erfolgen direkte oder indirekte Transfers in Drittstaaten, wie u. a. USA, Indien oder China? Hinweis: • Für die EU und die USA gilt der Angemessenheitsbeschluss basierend auf dem Datenschutzrahmen (EU-US Data Privacy Framework) (seit 10. Juli 2023)	• Wie sind die Vereinbarungen über die Weitergabe von IT-Diagnose-Daten geregelt? • Welches Recht gilt? Ist es DSGVO- bzw. DSG-konform? • Ist der Hersteller im Falle der USA unter *https://www.dataprivacyframework.gov/list* gelistet? • Werden die Daten eventuell aus diesem Land in weitere nachfolgende Drittländer übertragen, z. B. in die dortigen Labore und Supportzentren der Hersteller (z. B. von USA nach Indien oder China)?

3 Prüfkatalog »I«: »Inhouse-Handhabung« von IT-Diagnose-Daten

IT-Diagnose-Daten stellen ggf. auch dann ein Risiko dar, wenn sie zwecks Analyse inhouse mit anderen Abteilungen geteilt werden, insbesondere im Falle von Produktionssystemen. Die Relevanz einer Prüfung ergibt sich aus dem Vorhandensein einer eigenen Softwareentwicklung. Entsprechende Anforderungen gelten aber auch bei einer ausgelagerten Softwareentwicklung.

ID	Prüfthema	Ausprägung
I.01	Wie ist der Zugang zu IT-Diagnose-Dokumenten für die firmeneigene Softwareentwicklung geregelt? Hinweise: • Initial entscheidend für die notwendige Risikoklassifizierung ist die Lokation der Entwicklungsabteilung. Ist diese wirklich inhouse oder near- oder gar offshore? • Im Zweifelsfall sollte auch eigenen Entwicklern nur Zugriff auf bereinigte Dokumente aus der Produktionsumgebung gewährt werden.	• Bestehen Regelungen zum Zugriff der eigenen Softwareentwickler auf IT-Diagnose-Daten aus der Produktion? • Differenzieren die Regelungen nach Test-, Entwicklungs- und Produktionsumgebung (siehe I.03)?
I.02	Sind Teile der Entwicklung bzw. des Inhouse-Supports ausgelagert, z. B. off- oder nearshore? Hinweis: • In diesem Fall verläuft die Risikoeinschätzung analog zu einem externen Softwarehersteller.	• Sind die Risiken um die Dienstleister konkret und individuell evaluiert worden?
I.03	Sind eventuelle Abweichungen für Test, Entwicklung und Produktion klar geregelt? Hinweis: • Siehe auch G.02.	• Sind in jedem Fall strenge Regelungen für IT-Diagnose-Daten aus der Produktion getroffen worden?
I.04	Sind die Zugriffsrechte für IT-Diagnose-Dokumente auf den einzelnen Betriebssystemen für Entwickler restriktiv geregelt? Hinweis: • Siehe auch G.07.	• Ist in jedem Fall das produktive Umfeld restriktiv reglementiert?

→

ID	Prüfthema	Ausprägung
I.05	Wird für die eigenen Anwender ein interner First-/Second-Level-Support oder ein Helpdesk betrieben, der auf IT-Diagnose-Daten zugreift? Hinweis: • In diesem Fall herrschen quasi Verhältnisse wie bei einem Softwarehersteller, und die Dokumente sind zu bereinigen.	• Haben dessen Mitarbeiter Zugriff auf IT-Diagnose-Daten?

4 Prüfkatalog »K«: Transparente Kommunikation der Bereinigung gegenüber relevanten Parteien

Der praktizierte risikominimierende Umgang mit IT-Diagnose-Daten sollte gegenüber verschiedenen Parteien proaktiv kommuniziert werden.

ID	Prüfthema	Ausprägung
K.01	Wird im Unternehmen in den betroffenen IT-Bereichen die notwendige Awareness über die Risiken von IT-Diagnose-Daten betrieben? Hinweis: • Dies betrifft Administratoren sowie Infrastruktur- und Applikationsverantwortliche, aber auch hauseigene Entwickler.	• Werden alle Parteien im IT-Betrieb regelmäßig über die Risiken von IT-Diagnose-Daten informiert? • Wie sieht die Awareness konkret aus? • Werden externe Mitarbeiter gleichfalls auf das Thema hingewiesen? • Existieren z. B. Informationsmaterial, Rundschreiben oder Sitzungsprotokolle als Nachweis für Awareness-Maßnahmen?
K.02	Wird die Tatsache der Bereinigung gegenüber den Empfängern, d. h. den Softwareherstellern, offen kommuniziert? Hinweise: • Dies kann wichtig sein, weil eine verfälschte IP-Adresse z. B. nach außen so wirkt wie eine echte. Um eventuelle Zweifel während der Analyse zu vermeiden, sollten alle verfälschten IDs etc. als Liste bereitgestellt werden. Eine entsprechende Liste muss die Bereinigungslösung automatisch erzeugen. • Es ist wichtig festzuhalten, dass durch das Bereitstellen der Liste verfälschter IDs keine Pseudonymisierung resultiert. Es wird nicht die vollständige Übersetzungstabelle übergeben, sondern nur eine Spalte davon.	• Wird der Empfänger über die Tatsache bereinigter IT-Diagnose-Daten deutlich informiert? • Wird den Herstellern für eine optimale Arbeit auch eine Liste verfälschter IDs, IP-Adressen etc. bereitgestellt?
K.03	Ist der Fall geregelt, wenn Hersteller mit den bereinigten Dokumenten nicht vollständig zurechtkommen? Zum Beispiel wenn wider Erwarten Einsicht in Daten aus bereinigten Bereichen benötigt wird. Hinweise: • Die wesentlichen Entscheidungsparameter sind die Größe der einzusehenden Bereiche und die Sensibilität der darin enthaltenen Daten. • Es darf z. B. nicht sein, dass als Reaktion pauschal das gesamte Originaldokument gesendet wird.	• Sind die notwendigen Schritte für diesen Fall festgelegt und dokumentiert? • Sind ein Genehmigungsprozess und die notwendigen Detailprüfungen definiert? • Ermöglicht es die angewandte Bereinigungslösung, a) Auskunft über die in diesen Bereichen enthaltenen Daten zu geben und b) eine zweite Variante eines Dokuments zu erstellen, in der diese ausgewählten Bereiche wieder im Original vorliegen?
K.04	Wurde die Cyber-Insurance-Police bezüglich möglicher Obliegenheiten in Bezug auf den Umgang mit IT-Diagnose-Daten geprüft? Hinweis: • Es ist zu empfehlen, die eigene Cyber-Insurance über die praktizierte Bereinigungsmethode, wie z. B. Anonymisierung, proaktiv und explizit zu unterrichten; spätestens im Fragebogen des nächsten Risikoreviews.	• Ist in offener Kommunikation klargestellt, dass bei »vorbildlichem« Umgang mit IT-Diagnose-Daten eine Obliegenheitsverletzung oder Gefährdungserhöhung, mit eventueller Folge der Deckungseinschränkung, ausgeschlossen werden kann?

→

ID	Prüfthema	Ausprägung
K.05	Wird im Falle eines externen Audits durch Wirtschaftsprüfer oder im Rahmen einer Zertifizierung (PCI, ISO o. ä.) über die positiven Maßnahmen im Umfeld von IT-Diagnose-Daten offen gesprochen?	• Wird der risikobewusste Umgang mit IT-Diagnose-Daten auch gegenüber externen Auditoren proaktiv dargestellt?

5 Prüfkatalog »E«: IT-Diagnose-Daten im Falle der Inanspruchnahme von Cloud-, Hosting- oder Application-Providern

Bei Inanspruchnahme externer Infrastruktur- und Applikationsdienstleister ist eine Prüfung der datenschutzrechtlichen Vereinbarungen, unabhängig vom speziellen Fokus IT-Diagnose-Daten, elementar. Diese Prüfung erfolgt meistens bereits im Rahmen der Beauftragung. Zu den speziellen Vereinbarungen zählen die klaren Regelungen, Absprachen und Erwartungshaltungen im Umgang mit IT-Diagnose-Daten. Ergänzende Prüffragestellungen, z. B. im Falle des Outsourcings oder der Cloud-Nutzung, haben zum Ziel, dass in externen IT-Bereichen dieselben hohen Standards herrschen wie intern.

ID	Prüfthema	Ausprägung
E.01	Ist mit externen Dienstleistern der Umgang mit IT-Diagnose-Daten von den für Kunden betriebenen Systemen und Anwendungen klar geregelt? Dies gilt insbesondere für Systeme und Applikationen, auf/mit denen die Kundendaten verarbeitet werden. Hinweise: • Ein präventiver Ansatz kann vorsehen, dass der Kunde die Bereinigung selbst vornimmt und der Dienstleister die Dokumente dann für den Upload zurückerhält. Letztlich wäre die Verantwortung auf diese Weise »lupenrein« geregelt und abgegrenzt. • Hintergründe und Vorteile dieser Strategie: a) Nur der Kunde weiß wirklich über das in der eigenen IT vorkommende sensible Datenspektrum exakt Bescheid, b) fremde Dienstleister kümmern sich nicht um »fremde Geheimnisse«, sondern machen ihren Job im eigentlichen Leistungsbereich, und c) man lebt die Wichtigkeit des Datenschutzes aktiv und praktisch vor (Awareness).	• Werden grundsätzlich die Anforderungen analog zum Prüfkatalog »G« auch bei Inanspruchnahme eines Dienstleisters eingehalten? • Ist dies im Rahmen der Beauftragung oder nachträglich entsprechend vereinbart worden?
E.02	Besteht bei den Systemadministratoren der externen Provider ausreichend faktische Awareness bezüglich der Risiken um IT-Diagnose-Daten? Hinweise: • Bloße »Paper-based Compliance« ist einfach zu erreichen. Aufgrund des Gefälles zwischen Brisanz der Daten und potenzieller Arglosigkeit der Provider-Mitarbeiter gilt das Prinzip »Wehret den Anfängen«, und zwar durch eine explizite Adressierung des Themas gegenüber den Provider-Mitarbeitern. • Das Problem besteht in der Intransparenz der Provider-internen Strukturen und dem fehlenden direkten Zugang zum Personal – ganz zu schweigen von einer Weisungsbefugnis.	• Wird beispielsweise auf ein Awareness-Video oder aufklärende Dokumente verwiesen, verbunden mit einer Verpflichtung zur Bestätigung der Kenntnisnahme?
E.03	Ist der Zugriff auf IT-Diagnose-Daten auch auf den ausgelagerten Systemen klar definiert?	• Werden grundsätzlich die Anforderungen analog zum Prüfkatalog »G« auch bei Inanspruchnahme eines Dienstleisters eingehalten?

6 Stichprobenbasierte Prüfung »S« des korrekten Umgangs mit IT-Diagnose-Daten

Der Ablauf einer stichprobenbasierten Überprüfung der Einhaltung aller Regelungen kann sich wie folgt gestalten:

Schritt	Prüfaktion	Ausprägung
S.01	Erhebung einer Einstiegsstichprobe von Herstellern bzw. Providern und deren Ticketsystemen.	• Ermittlung einer Liste der Hersteller und Dienstleister und Auswahl von mindestens drei bis fünf IT-Diagnose-Daten-relevanten Kandidaten. • Berücksichtigung von kleinen und mittelgroßen Softwareherstellern, nicht nur Big Player. Damit ist auch der Fall abgedeckt, dass der Hersteller kein Problem-Management-Portal betreibt. • Einbeziehen eines in den USA oder einem anderen Drittland ansässigen Herstellers (siehe S.08). In jedem Fall ist zu fragen, ob es Hersteller ohne europäische Repräsentanz gibt. • Analyse der Zusammenarbeit mit den ausgewählten Softwareherstellern anhand der Problem-Management-Portale (»Ticketsysteme«) bzw. E-Mail-Kommunikation, z. B. anhand zweier Beispiele pro Kandidat.
S.02	Auswahl z. B. zwei oder drei beispielhafter Vorgänge (»Cases«) pro ausgewähltem Hersteller bzw. Provider, die einen Upload von IT-Diagnose-Dokumenten beinhalten – vorzugsweise Dumps. Diese Stichprobe ist detailliert zu prüfen.	• Es werden Fälle aus unterschiedlichen Ticketsystemen gewählt, also von unterschiedlichen Herstellern. • Auch hier gilt: Einbeziehen eines kleineren Softwareherstellers, Analyse der Details des Uploads und die Einhaltung der Regelungen anhand von Problem-Tickets, z. B. von K.02. Anhand der Dateinamen kann ggf. bereits erkannt werden, ob die Originaldateien oder die bereinigten Fassungen gesendet wurden.
S.03	In einem ersten Schritt sollten für zwei Vorgänge die Begleitdokumente zu den Bereinigungen und die eventuell vorhandenen Löschungsbestätigungen vorgelegt werden.	• Prüfung der Eintragungen in den eigenen übergreifenden Aufzeichnungen (siehe G.06). • Prüfung anhand der Dokumente, ob der Katalog von sensiblen Datentypen tatsächlich bereinigt wurde. Entspricht dieser den Vorgaben gemäß G.10?
S.04	Gibt es Vorgänge, in denen nachträglich »unbereinigte«, d. h. Originalbereiche, »nachbestellt« wurden?	• Prüfung dieser Vorgänge und Begleitdokumente.
S.05	Nachvollzug der transparenten Kommunikation vollzogener Bereinigungen gemäß Prüfkatalog »K«.	• Wird dem Empfänger gegenüber klar und sichtbar erwähnt, dass die erhaltenen Daten bereinigt sind? • Wurde eine Liste der verfälschten Daten bereitgestellt, z. B. über verfälschte IP-Adressen? Diese Liste darf nicht einer Pseudonymisierungsliste entsprechen.
S.06	Der Vorgang der Bereinigung sollte einmal auf praktische Weise vorgeführt werden. Feststellung der voreingestellten und praktizierten Datentypen, nach denen gesucht wird.	• Demonstration der Bereinigung von Beispieldateien aller IT-Diagnose-Dokumenten-Typen, wie insbesondere Dumps, Logs und Traces. • Entspricht der Prozess den Vorgaben gemäß G.10? • Wo erfolgte die Bereinigung (siehe G.13)?
S.07	Ermittlung von dringenden Situationen, in denen Dokumente ggf. nur um eine reduzierte Menge an Datentypen bereinigt wurden.	• Erläuterung der Dringlichkeit in diesem Fall.
S.08	Erfolgen direkte oder indirekte Transfers in Drittstaaten, wie u. a. USA, Indien oder China?	• Manchmal haben Hersteller oder Provider keine Repräsentanz in Europa, und man arbeitet direkt mit dem Support im Drittstaat zusammen.
S.09	Wie erfolgt das Logging bei der Entstehung von IT-Diagnose-Daten?	• Beurteilung zum einen der »Buchhaltung« von IT-Diagnose-Daten (siehe G.06), aber auch der automatischen technischen Detektionen und Protokollierungen (siehe G.19).
S.10	Begleitung einer aktuellen Supportanfrage bei einem Hersteller.	• Ideal wäre es, wenn ein solcher Prozess, von der Erkennung des Problems über die Sichtung und Bereinigung der notwendigen IT-Diagnose-Daten bis hin zur Ticketerstellung sowie dem Transfer der Daten, begleitet und eingesehen werden könnte.

Literatur

[Fedtke 2023] *Fedtke, S.:* Nach Microsoft-Schlüssel-Diebstahl aus Crash-Dump – neues IT-Audit-Prüfthema: IT-Diagnose-Daten. IT-Governance Heft 38, 2023, 17. Jg., S. 22-27.

[Malek 2024] *Malek, P.:* Datenschutzrechtliche Haftungsrisiken nach Cyber-Vorfällen im Spiegel aktueller EuGH-Rechtsprechung. Die VersicherungsPraxis 2, Februar 2024, S. 3-6.

[Speichert 2023] *Speichert, H.:* DSGVO-Haftungs- und Sicherheitsrisiken durch Protokoll- und Diagnosedaten im IT-Betrieb. Datenschutz und Datensicherheit (DuD) 47, 04/2023, S. 229-232; *https://www.enterprise-it-security.com/DuD-Artikel-Speichert-042023/GOV.*

Stephen Fedtke

ist Wirtschaftsingenieur und CTO von ENTERPRISE-IT-SECURITY.COM, ein auf IT-Sicherheit und Compliance-Lösungen spezialisierter Dienstleistungsbereich des Unternehmens Dr. Stephen Fedtke System Software. Außerdem ist er Autor und Herausgeber im Verlag Springer Vieweg.

Dr. Stephen Fedtke
Enterprise-IT-Security.com
Seestr. 3a
CH-6300 Zug
Schweiz
stfedtke@enterprise-it-security.com
www.enterprise-it-security.com