2100

Informationstechnologie (IT)

- **Definition des Sachgebiets**
- **Fachliche Bestellungsvoraussetzungen**

Anlage 1: Darstellung der Sachgebietseinteilung
Anlage 2: Merkblatt zum Sachgebiet „IT – Schwerpunkt Software, insbesondere IT-Forensik“

Stand: März 2015
Revisionsnummer: 4
Erste Fassung: vor 1983

DIHK Deutscher Industrie- und Handelskammertag

I. Allgemeine Gliederung

1. Sachgebietseinteilung und Bestellungstenor

Die Informationstechnologie (IT) hat nahezu alle Wirtschafts- und Lebensbereiche durchdrungen und besitzt damit eine wichtige Querschnittsfunktion. Fachliche Bestellungsvoraussetzungen müssen daher notwendigerweise sinnvolle Teilbereiche abgrenzen, gleichzeitig aber in geeigneter Weise solche Bereiche zusammenfassen, die von einer/einem einzelnen Sachverständigen abgedeckt werden können.

Die Einteilung des interdisziplinären Sachgebiets beruht auf den Begrifflichkeiten eines durchschnittlichen IT-Anwenders, der Sachverständigenleistungen nachfragt. Eine wissenschaftlich exakte Gliederung steht daher hinter dieser Praxisanforderung zurück. Die Inhalte der einzelnen Teilbereiche sind breit gefasst und offen formuliert, um dem schnellen technischen Fortschritt gerecht zu werden und den Interessenten an Sachverständigenleistungen einen Anhaltspunkt zu liefern, welche Sachverständige in einem spezifischen Anwendungsbereich Leistungen erbringen können. Angestrebt wurde eine herstellerunabhängige und produktneutrale Formulierung, so dass neue Entwicklungen möglichst unmittelbar aufgefangen werden können.

Die Sachgebietseinteilung berücksichtigt, dass kein/e Sachverständige/r auf dem gesamten Gebiet der Informationstechnologie gleichermaßen besonders sachkundig sein kann, weshalb das Sachgebiet in die beiden Schwerpunkte „Hardware“ und „Software“ eingeteilt ist. Dementsprechend lauten die grundlegenden Möglichkeiten des Bestellungstenors:

„IT - Schwerpunkt Hardware“
„IT - Schwerpunkt Software“

Dabei stehen die beiden Schwerpunkte nicht isoliert nebeneinander, sondern überschneiden sich. Oftmals wird erst im Rahmen der Begutachtung durch eine/n Sachverständige/n deutlich, welchem Schwerpunkt die aufgetretenen Probleme zuzuordnen sind. Um eine gutachterliche Fragestellung ganzheitlich betrachten und lösen zu können, muss jede/r Sachverständige daher gewisse Grundkenntnisse auch im jeweils anderen Schwerpunkt besitzen.

Soweit ein/e Sachverständige/r darüber hinaus besondere Kenntnisse in einem Zusatzgebiet nachweist, kann dies - auf Antrag - im Bestellungstenor mit dem Zusatz „insbesondere...“ mit der Bezeichnung des Zusatzgebietes kenntlich gemacht werden. Derzeit bestehen folgende Zusatzgebiete, welche die oben genannten Anforderungen erfüllen und eine hinreichende Breite aufweisen:

Zusatzgebiete beim Schwerpunkt Hardware:
* Audio- und Videotechnik
* Automotive
* Industrieelektronik und Steuerungstechnik
* Mobile Endgeräte
* Netzwerke und Telekommunikation
* Rechenzentren

Zusatzgebiete beim Schwerpunkt Software:
* Anwendungen für mobile Endgeräte
* eBusiness
* Enterprise Resource Planning (ERP)
* IT-Forensik
* IT-Sicherheit

Trend-Begriffe wie Big Data, Cloud-Computing, Webshop sind bewusst nicht als Zusatzgebiete vorgesehen, da nicht zu erwarten ist, dass diese von Dauer sind.

Eine Darstellung der Sachgebietseinteilung befindet sich in Anlage 1.

Es ist möglich, die genannten Zusatzgebiete im Tenor zu führen. Auch die Tenorierung von Teil-Zusatzgebieten ist möglich, sofern es sich um praxisgerechte, eindeutig abgrenzbare Teil-Zusatzgebiete handelt.

Beispiele für mögliche Tenorierungen mit Bezug auf die genannten Zusatzgebiete:

"IT - Schwerpunkt Hardware, insbesondere Mobile Endgeräte"
"IT - Schwerpunkt Software, insbesondere IT-Forensik"

Beispiele für mögliche Tenorierungen mit Bezug auf Teil-Zusatzgebiete:
„IT - Schwerpunkt Hardware, insbesondere Funkanlagen“
„IT - Schwerpunkt Hardware, insbesondere Gebäudeautomation“

Die Einteilung berücksichtigt somit das Bedürfnis der Nachfrager von Sachverständigenleistungen, das fachliche Problem nicht exakt benennen zu müssen. Vielmehr besteht aufgrund der Breite und der verständlichen Bezeichnung der Schwerpunktbereiche und Zusatzgebiete eine hinreichende Gewissheit dafür, dass ein/e Sachverständige/r die Aufgabenstellung qualifiziert und sachgerecht bearbeiten kann.

Das Sachgebiet „Informationstechnologie (IT)“ ist abzugrenzen zu folgenden anderen Sachgebieten:
- Elektrotechnische Anlagen und Geräte
- Bestimmung der Exposition durch elektromagnetische Felder (EMF)
- Überprüfung von Geldspielgeräten
- Telekommunikation im Bereich Verbindungspreisberechnung

.

2. Vorbildung und praktische Tätigkeiten

2.1. Erforderlich ist entweder
ein erfolgreich abgeschlossenes Studium mit einer Regelstudienzeit von mindestens sechs Fachsemestern an einer Hochschule nach dem Hochschulrahmengesetz in den Fachrichtungen
- Informatik/Wirtschaftsinformatik
- Ingenieurwissenschaften
- Wirtschaftswissenschaften
- Wirtschaftsingenieurwissenschaften
- Physik
- Mathematik

bzw. entsprechende Kombinationen und eine mindestens fünfjährige praktische Tätigkeit, die ihrer Art nach geeignet war, die erforderlichen Kenntnisse zu vermitteln,

oder
bei Antragstellerinnen/Antragstellern ohne entsprechenden Hochschulabschluss der Nachweis von Erfahrung, Aus- und Fortbildung sowie regelmäßig einer 10-jährigen praktischen Tätigkeit, die ihrer Art nach geeignet sind, die erforderlichen Kenntnisse zu vermitteln.

2.2. In allen Fällen muss die/der Antragsteller/in nachweisen, dass sie/er in fachverantwortlicher Stellung im Bereich der IT tätig ist. Sie/er sollte sich mit Themen wie z. B.

Zeit, Kosten, Qualität, Markt, Branchenüblichkeit, Stand der Technik auseinandergesetzt haben. Das erforderliche Erfahrungsniveau wird u. a. durch folgende Tätigkeiten gekennzeichnet:

- Umfassende Systementwicklungen auf dem entsprechenden Schwerpunktgebiet
- Erarbeitung umfangreicher Dokumentationen
- Erarbeitung umfangreicher Pflichtenhefte
- Projektmanagement für anspruchsvolle Aufgaben
- Erstellung von Gutachten oder vergleichbaren schriftlichen Ausarbeitungen.

2.3. Die/der Antragsteller/in soll eine mindestens dreijährige einschlägige praktische Tätigkeit als Sachverständige/r nachweisen. Diese Tätigkeit darf - vom Zeitpunkt der Antragstellung an gerechnet - nicht länger als ein Jahr zurückliegen.

2.4. Die vorerwähnten Voraussetzungen sind durch Vorlage von mindestens fünf Gutachten nachzuweisen. Sofern die/der Antragsteller/in zusätzlich eine öffentliche Bestellung in einem Zusatzgebiet der IT („IT – Schwerpunkt Software, **insbesondere ……**“ beziehungsweise „IT – Schwerpunkt Hardware, **insbesondere ……**“) beantragt, müssen sich zwei der fünf einzureichenden Gutachten auf das Zusatzgebiet beziehen. In begründeten Einzelfällen können zwei Gutachten durch vergleichbare Ausarbeitungen, zum Beispiel Veröffentlichungen, ersetzt werden.

Auf das Merkblatt „Empfehlungen für den Aufbau eines schriftlichen Sachverständigengutachtens“ wird verwiesen.
(https://www.muenchen.ihk.de/de/recht/Anhaenge/aufbau-eines-sachverstaendigengutachtens.pdf)

3. Allgemeines

Antragsteller/innen müssen zum Nachweis der besonderen Sachkunde Kenntnisse in den jeweils angegebenen Vertiefungsgraden nachweisen:
Grundkenntnisse (G)
Vertiefte Kenntnisse (V)
Detailkenntnisse (D)

Die bei den Fachkenntnissen (Ziff. 5) und Zusatzgebieten (Ziff. 6) in Klammern angegebenen Beispiele dienen lediglich zur Erläuterung. Sie erheben keinen Anspruch auf Vollständigkeit.

4. Allgemeine Kenntnisse

4.1. Rechtsgrundlagen

Die „Rechtskenntnisse Sachverständigentätigkeit“ in der jeweils gültigen Fassung sind Bestandteil dieser Bestellungsvoraussetzungen.

Darüber hinaus sind folgende spezielle Rechtskenntnisse nachzuweisen:
a) einschlägige versicherungsrechtliche Vorschriften (G)
b) einschlägige Vorschriften des Ordnungswidrigkeitenrechts (G)
c) einschlägige Vorschriften des Strafrechts (§§ 11 Abs. 3, 184 a-d, 202 a-c, 206, 263a, 266b, 268, 269, 270 StGB) (G)
d) weitere einschlägige Straftatbestände (UWG, UrhG, HGB, AO) (G)

e) forensisches Vorgehen bei Datensicherung und Auswertung (Umgang mit Beweismitteln, Anfertigung von Kopien, Prüfsummen, Protokollierung) (G)
f) Datenschutzgesetze (V)

4.2. Wert- und Kostenbegriffe im Sachverständigenwesen

Die einschlägigen Wert- und Kostenbegriffe müssen bekannt sein (vgl. Glossar „Wert- und Kostenbegriffe“ https://www.muenchen.ihk.de/de/recht/Anhaenge/wert-und-kostenbegriffe-im-sachverstaendigenwesen.pdf).

5. Fachkenntnisse

Von der/dem Sachverständigen wird erwartet, dass sie/er vor allem Störungs- und Ausfallmechanismen innerhalb des gesamten Spektrums ihres/seines Sachgebietes kennt und aufgrund ihres/seines systematischen Fachwissens ermitteln und nachvollziehbar beschreiben und bewerten kann.

Sachverständige müssen in ihrem Schwerpunkt über folgende Kenntnisse verfügen:

Sachverständige müssen in ihrem Schwerpunkt über folgende Kenntnisse verfügen:

a) Allgemein anerkannte Regeln der Technik (D)
b) Stand der Technik (D)
c) marktgängige Standards (V)
d) verbreitete Produkte (V)
e) Branchenüblichkeit (V)
f) Entwicklungstendenzen (V)

5.1. Schwerpunkt Hardware

5.1.1. Grundlagenwissen (G)

a) Physik (grundlegende Begriffe und Gesetze der Elektrodynamik, Optik, Akustik, Mechanik)
b) Elektrotechnik (Ströme und Spannungen in elektrischen Netzwerken, Wechselstromtechnik, Filterschaltungen, Schwingkreise, elektrische und magnetische Felder)
c) Werkstoffe (physikalisch-chemische Materialeigenschaften von Metallen, Halbleitern, Isolatoren)
d) Messtechnik (elektrische Messung physikalischer Größen, Prinzip und Aufbau von Messsystemen, Systemoptimierung und Fehlerkorrektur, Standard-Messgeräte)
e) Mathematik (Logische Grundlagen (Bool'sche Algebra))

5.1.2. Hardware

5.1.2.1. Bauelemente (V)

Aufbau, Wirkungsweise und Dimensionierung der wesentlichen elektrischen und elektronischen Bauelemente:

a) passive Bauelemente (Widerstände, Kondensatoren, Induktivitäten, Varistoren, Sensoren)

b) aktive Bauelemente (diskrete Halbleiterbauelemente, integrierte Schaltungen, Mikroprozessoren, Speicher/Peripherie, CCD-Elemente, optoelektronische Bauele-mente)
c) elektromechanische Bauelemente (Relais, Schalter, Steckverbindungen, Leiterplatten, Kabel)

5.1.2.2. Baugruppen/Geräte (V)
Technologie, Aufbau und wesentliche Funktionen von Baugruppen und Geräten der Informationstechnologie:
a) Rechner-/Steuereinheiten
   aa) Prozessortypen und Kennwerte
   bb) Speichersysteme
   cc) Bus-Systeme
   dd) Schnittstellen
   ee) Montage, Verkabelung
   ff) Speicherprogrammierbare Steuerung (SPS)
b) Peripherie
   aa) Massenspeicher (Festplatte, Band, CD, DVD, Halbleiter)
   bb) Eingabegeräte (Lesegeräte, Scanner)
   cc) Ausgabegeräte (Drucker, Displays)
   dd) Video- und Audiogeräte

5.1.2.3. Netzwerktechnik (V)
a) Übertragungsverfahren
b) Topologien
c) Komponenten (Hub, Switch, Router)
d) Signalübertragung (physikalische und logische Ebenen)

5.1.2.4. Betrieb von Geräten und Anlagen (V)
a) Erforderliche Energieversorgung (Schutzmaßnahmen)
b) Erforderliche Umgebungsbedingungen, Kühlung
c) Schäden an Geräten/Anlagen (Überspannung, Wasser, Feuer, Staub)
d) Sanierung von Schäden an Geräten und Anlagen
e) Elektrische Störungen in Art, Entstehung, Ausbreitung und Wirkung (EMV)

5.1.3. Software (G)
a) Rechnerarchitekturen/Peripherie
b) Betriebssysteme (Embedded, Real Time Operating Systems)
c) Microcode (Firmware), Assembler
d) Datensicherheit (Zugriffsschutz, Übertragungssicherheit, Kryptographie)
e) Datensicherung (Verfahren, Lagerung, Datenrettung)
f) Netzwerke (LAN, WAN, Internet)
g) Bedrohungen (Hacking, Viren) und Schutzmechanismen (Firewall)
h) Audio, Video, Grafik
i) Datenverwaltung
j) Protokolle

5.2. Schwerpunkt Software

5.2.1. Grundlagenwissen

5.2.1.1. Informationstechnik (G)

a) Grundlagen (Berechenbarkeit, Grammatiken, Komplexitätstheorie, Informationsgehalt, Logik)
b) Modellierung (Abstraktion, Graphen, Strukturen, Prozesse)
c) Querschnittsverfahren (IT-Sicherheit, Qualitätssicherung)
d) Programmierparadigmen
e) Algorithmen und Datenstrukturen

5.2.1.2. Betriebswirtschaft (G)

a) Grundbegriffe (Wirtschaftlichkeit, Aufwand und Ertrag)
b) Unternehmensaufbau und Management (Organisation, Geschäftsprozesse, Finanzen, Investitionsrechnung, internes und externes Rechnungswesen, Einkauf, Leistungserstellung, Materialwirtschaft, Vertrieb, Service und Marketing)

5.2.2. Software

5.2.2.1 Software Engineering

a) Agile und herkömmliche Vorgehensmodelle (D)
b) Spezifikationsmethoden (D)
c) Programmiersprachen (V)
d) Technischer Systementwurf (V)
e) Arten der Dokumentation (V)
f) Datenbankentwicklung und Datenbankdesign (D)
g) Qualitätssicherung / Test (D)
h) Datenmigration (V)
i) Projektmanagement (D)
j) Schnittstellen (V)
k) Entwicklungsumgebungen (D)
l) Software-Engineering-Werkzeuge (D)
m) Systemumgebungen (V)
n) Systemarchitekturen (D)
o) Requirements Engineering (V)
p) Change Request-Verfahren (V)

5.2.2.2. Systemsoftware (V)

a) Betriebssysteme (Prozesse, Verteilte Systeme, Client-Server-Systeme, Synchronisation, Unterscheidungsmerkmale aktueller Systeme)
b) Datenbankmanagementsysteme (DBMS) (Datenbankmodelle, Abfragesprachen, Transaktionsverwaltung, Datenintegrität, Data Warehouses)
c) Middleware
d) Virtualisierungssysteme

5.2.2.3. Einsatz von Software (V)

a) Standardsoftware (branchenübergreifende Lösungen, branchenspezifische Lösungen, ERP-Systeme, E-Commerce-Lösungen, Einführung)
b) Individualsoftware (Einführung)

c) Pflege und Wartung (Support-Organisation, Konfigurationsmanagement)
d) Dokumentation
e) Projekte (Organisation und Projektmanagement, Abnahme, Vorgehensmodelle)
f) Systemgestaltung (Usability, Gestaltungsprozesse)
g) Systemintegration und Schnittstellen
h) Auswirkungen des IT- Einsatzes (Folgen, Risiken und Gefährdungspotentiale)
i) Unternehmensübergreifende Software (CRM, SCM, EDI, EDIFACT)
j) Internet-Kommunikation (E-Mail, FTP, Chat, Messaging)

5.2.3. Betrieb von Systemen (Rechenzentren, Administration) (V)

a) IT Service Management Best Practices
b) Service Level Agreements
c) Leistungs- und Abrechnungsformen
d) Fragestellungen bei Outsourcing und externer Datenspeicherung (organisatorisch, rechtlich)
e) Konfigurationsmanagement
f) Betrieb komplexer Systeme

5.2.4. Hardware (G)

a) Computer (Rechnerorganisation, Rechnerarchitektur)
b) Peripheriegeräte (Speichersysteme, Datenein- und -ausgabegeräte)
c) Datenübertragung und Vernetzung (Konzepte, Möglichkeiten und Verfahren zur Verbindung von Standorten, Daten- und Telekommunikation)
d) Fehlertoleranz (Verfügbarkeit, technische Möglichkeiten)
e) Energieversorgung und Elektrotechnik (im Zusammenhang mit Hardwarekomponenten und Datenübertragung)

6. Zusatzgebiete

6.1. Schwerpunkt Hardware

6.1.1. Audio- und Videotechnik

Audio- und Videotechnik haben sich aus ihrem klassischen Bereich der Ton- und Bildaufzeichnung hin zu komplexen Systemen entwickelt, z.B. für industrielle Qualitätssicherung, für Zutrittskontrolle oder Objektschutz. Software spielt hierbei eine zunehmende Rolle.

a) Hardware (V)
   aa) Aufnahmegeräte (Audio/Video)
   bb) Aufzeichnungsgeräte (Audio/Video)
   cc) Schnittstellen
   dd) Managementsysteme
   ee) Datenformate
   ff) Kompressionsverfahren
   gg) Übertragungsverfahren/Normen

b) Software (V)
   aa) Verschlüsselungsverfahren
   bb) Streamingverfahren

cc) Videosensorik
dd) Analysemodule
ee) Biometrische Verfahren
ff) Bildbearbeitung
gg) Konferenzsysteme

c) Betrieb von Anlagen (V)
aa) Datenschutz
bb) Betrieb von Sicherheitsanlagen

6.1.2. Automotive

Im Zusatzgebiet "Automotive" geht es im Wesentlichen um die Funktion, Wirkung, Fehler und Mängel der Steuergeräte, die in Fahrzeugen eingebaut sind. Steuergeräte gibt es für die unterschiedlichsten Aufgaben und mit völlig unterschiedlicher Leistungsfähigkeit. Beispiele sind: Tastenmodule, intelligente Sensoren, Motorsteuergeräte, sicherheitsrelevante Steuergeräte und Assistenzsysteme, Einparkassistent, Navigation-, Video-Audio-Systeme.

a) Fahrzeugzustand und Verhalten der Steuergeräte (D)

b) Hardware
aa) Aufbau der Steuergeräte (Sensoren, Steckverbindungen) (D)
bb) Microcontroller (G)
cc) Bus-Technologie (V)
dd) Funktion und Schnittstellen von Sensoren und Aktoren (V)
ee) Spannungsversorgung in Fahrzeugen (D)
ff) Umwelteinflüsse auf Elektronik in Fahrzeugen (D)

c) Diagnose und Einstellmöglichkeiten von Steuergeräten (V)
aa) Diagnosegeräte
bb) Sicherheit und Manipulationsmöglichkeiten

d) Software (G)
aa) Struktur und Aufbau der Software der Steuergeräte
bb) Funktionale Sicherheit

6.1.3. Industrieelektronik und Steuerungstechnik

Nahezu alle mit elektrischem Strom betriebenen technischen Geräte haben elektronische Steuerungen. Meistens verfügen sie über einen Prozessor, der mit eigener Software gesteuert wird, ohne dass dies ohne weiteres erkennbar wäre. Das Zusatzgebiet umfasst daher auch Gebäudeautomation, Prozessautomation sowie Mess-, Regelungs- und Steuerungstechnik (MSR).

Häufig werden Elektronikteile bis an die Grenzen der Spezifikation ausgereizt. Aus Kostengründen wird bei den Geräten meist wenig Sicherheitsspielraum eingebaut. Gleichzeitig sind die elektrischen Versorgungsnetze viel störungsbehafteter als früher. Durch europäische und internationale Vorschriften werden zunehmend enge Grenzen

bzw. genaue Definitionen für den Betrieb von elektrischen Geräten und Anlagen gesetzt. In diesem Spannungsfeld müssen sich Sachverständige sicher bewegen können.

a) Allgemeines
   aa) Physik, Chemie der Einsatzbereiche (G)
   bb) Werkstoffe (V)
   cc) Elektrische Messtechnik (D)
   dd) Elektrotechnische Grundlagen (V)

b) Bauelemente
   aa) Aktive und passive Bauelemente (D)
   bb) Sensoren (V)
   cc) Elektromechanische Bauelemente (D)

c) Systeme
   aa) Feldbus-Systeme (V)
   bb) Ethernet und Komponenten (V)

d) Software
   aa) Betriebssysteme (V)
   bb) Firmware (V)

e) Messtechnik
   Messung elektrischer Größen (D)

6.1.4. Mobile Endgeräte

Dieses Zusatzgebiet konzentriert sich auf die technischen Komponenten mobiler Endgeräte wie z.B. SmartPhones, PDAs, Tablets, eBook-Reader, Navigationsgeräte. Sachverständige müssen Funktionsweise und mögliche Mängel aller Baugruppen mobiler Endgeräte kennen. Außerdem sind Kenntnisse über die elektronischen Komponenten sowie über deren Verwendung und Zusammenwirken mit dem Einsatzumfeld erforderlich.

a) Standards
   aa) Mobilfunkdienste und deren Technik (u.a. GSM, UMTS, GPRS) (V)
   bb) GPS-Technologie (V)
   cc) Kommunikationstechnologien (WLAN, Bluetooth, NFC, USB) (D)
   dd) Internetprotokolle (TCP/IP, VPN, HTTP(S), TLS, SMTP, POP3, IMAP) (G)
   ee) Nachrichtentechnologien (SMS, MMS, E-Mail) (G)

b) Hardware (SmartPhones, PDAs, Tablets, eBook-Reader, Navigationsgeräte) (V)
   aa) Touchscreens
   bb) Prozessoren
   cc) Speichertechnik
   dd) Schnittstellen
   ee) Kameras
   ff) Sensoren
   gg) Antennen
   hh) Akkumulatoren

c) Betriebssysteme
   aa) Funktionsweise, Sicherheit und Systemarchitektur (Android, iOS, Windows Mobile / Phone, Symbian, Blackberry) (V)
   bb) Entsperren von Nutzungsbeschränkungen (Jailbreak, Rooting) (V)
   cc) Softwareentwicklung / Distribution von hardwarenahen Anwendungen (Firmware, Schnittstellen) (G)

d) Anwendungen (G)
   aa) Kurznachrichtendienste und Messenger
   bb) Multimedia-Apps (Audio- und Video-Player)
   cc) Standardanwendungen (Kalender, Kontakte, E-Mail)

6.1.5. Netzwerke und Telekommunikation

Netzwerke spielen im heutigen Informationsverarbeitungsprozess eine zentrale Rolle. Ihre Bedeutung und Anwendungsbreite wachsen ständig. Sachverständige müssen Kenntnisse in allen Netzwerkschichten haben. Beispiele sind die Auslegung eines Funknetzes, die Verknüpfung internationaler Unternehmensstandorte, Anforderungen bei der Nahfeld-kommunikation (NFC, RFID) und Next Generation Networks (NGN).

Das Zusatzgebiet umfasst auch Telekommunikationsanlagen, die jedoch aufgrund der fortschreitenden Technik an Bedeutung verlieren.

a) Kommunikationsmodelle Nachrichtenübertragungssysteme
   aa) Nachricht, Signal, Störgrößen (G)
   bb) OSI 7-Schichtenmodell (V)
   cc) Verkehrstheorie, Dämpfung, Pegelrechnung (V)
   dd) analoge/digitale Signalübertragung (V)
   ee) Raum-/Zeit-/Frequenzmultiplex (V)

b) Übertragungsmedien (Schicht 1)
   aa) elektrisch (Fernkabelnetz, Teilnehmeranschlussnetz, Breitbandkabelnetz, Busverkabelungen) (D)
   bb) optisch (Multimode, Single Mode, WDM) (V)
   cc) Funk (Frequenzspektren, Modulationsverfahren) (V)

c) Sicherungsmechanismen (Schicht 2)
   aa) Übertragungsverfahren (PDH, SDH, ATM, DOCSIS, xDSL, Ethernet, MPLS) (D)
   bb) Synchronisationsverfahren, Punkt zu Punkt - / Punkt zu Mehrpunkt-Technologien, Flusssteuerung, Überlastverhalten (D)
   cc) Authentifizierungsprotokolle, Verschlüsselung (D)

d) Vermittlungssysteme (Schicht 3)
Vermittlungsprotokolle (IPv4, IPv6, ICMP, IGMP,OSPF, BGP, SIP, ISDN, X.25) (D)

e) Transportsteuerung /-sicherung (Schicht 4)
Protokolle der Verbindungssteuerung (TCP, UDP, RSVP, Diffserv) (D)

f) Weitere Schichten

spezielle Funknetze (BOS) (V)

g) Bedrohungen, Forensik
Messtechnik, Protokollanalysatoren (Cace Pilot/Riverbed, Wireshark), Werkzeuge der Netzelemente (D)

h) Telekommunikationsanlagen (G)
aa) Telekommunikations-Endgeräte
bb) lokal vermittelnde Anlagen und Systeme
cc) Strukturen lokaler TK-Systeme
dd) Sicherheitskonzepte von ITK-Systemen
ee) Schutz gegen Überspannungseinflüsse

6.1.6. Rechenzentren

Als Rechenzentren werden sowohl Gebäude als auch Räumlichkeiten bezeichnet, in denen zentrale Informationstechnologie (Server, Storage, Netzwerk, Telekommunikationssysteme) betrieben wird. Zentraler Inhalt des Zusatzgebietes „Rechenzentren“ ist neben der Kenntnis der Funktion und Wirkungsweise der einzelnen Elemente ihre Differenzierung und das Erkennen möglicher Schwachstellen, die zu Fehlfunktionen führen können, inkl. der anzuwendenden Mess-/Nachweismethoden.

a) Energieversorgung der Rechenzentren
aa) Aufbau der primären und sekundären Stromversorgung der Rechenzentren (G)
Unterbrechungsfreie Stromversorgung (USV) (V)
Netzersatzanlagen (NEA) (V)
bb) Baugruppen der Stromversorgung (V)
cc) Bauelemente und Details der Stromversorgung (D)

b) Klimatisierung der Rechenzentren
aa) Grundlagen der Klimatisierung (Feuchtigkeit, Volumenstrom, Regelsysteme) (V)
bb) Aufbau und Funktion der Klimatisierung von Rechenzentren (G)
cc) Baugruppen der Klimatisierung (G)

c) Meldesysteme (Anforderungen) (G)
aa) Brandmeldeanlage (BMA)
bb) Einbruchsmeldeanlage (EMA)
cc) Gefahrenmeldeanlage (GMA)
dd) Alarmpläne

d) IT-Sicherheit
aa) Datensicherheit (V)
bb) Zutrittskontrolle (Vereinzelungsanlagen, Biometrie, Wachdienst, Kartensysteme) (V)

e) Bauliche Anforderungen (G)
aa) Brandschutz
bb) Einbruchschutz (Perimeterschutz, Video)
cc) Doppelboden (Druck, Öffnungen, Lüftungsbodenplatten, Flächenlast, Punktlast)
dd) Löschanlagen

f) Redundanzen (G)

g) Zertifizierung und Klassifizierung (G)

6.2. Schwerpunkt Software

6.2.1. Anwendungen für mobile Endgeräte

Sachverständige müssen Funktionsweise und mögliche Mängel von Anwendungen auf mobilen Endgeräten kennen. Dazu sind Kenntnisse über die spezifische Anwendungsentwicklung und das Zusammenwirken mit der Gerätehardware sowie dem Einsatzumfeld erforderlich.

a) Standards
   aa) Mobilfunkdienste und deren Technik (GSM, UMTS, GPRS) (G)
   bb) GPS-Technologie (G)
   cc) Kommunikationstechnologien (WLAN, Bluetooth, NFC, USB) (D)
   dd) Internetprotokolle (TCP/IP, VPN, HTTP(S), TLS, SMTP, POP3, IMAP) (V)
   ee) Nachrichtentechnologien (SMS, MMS, E-Mail) (D)

b) Hardware (SmartPhones, PDAs, Tablets, eBook-Reader, Navigationsgeräte)
   aa) Prozessoren (G)
   bb) Speichertechnik (D)
   cc) Schnittstellen (Bluetooth, Infrarot, NFC, USB) (G)
   dd) Kameras (G)

c) Betriebssysteme
   aa) Funktionsweise, Sicherheit und Systemarchitektur (Android, iOS, Windows Mobile / Phone, Symbian, Blackberry) (V)
   bb) Entsperren von Nutzungsbeschränkungen (Jailbreak, Rooting) (G)
   cc) Softwareentwicklung / Distribution von hardwarenahen Anwendungen (Firmware, Schnittstellen) (G)

d) Anwendungen
   aa) Kurznachrichtendienste und Messenger (D)
   bb) Multimedia-Apps (Audio- und Video-Player) (V)
   cc) Standardanwendungen (Kalender, Kontakte, E-Mail) (V)
   dd) Softwarearchitektur (V)
   ee) Sicherheit (V)
   ff) Entwicklungsumgebungen (D)
   gg) Distribution von Benutzeranwendungen (V)

6.2.2. eBusiness

Dieses Zusatzgebiet konzentriert sich auf den elektronischen Geschäftsverkehr. Sachverständige müssen die fachlichen Prozesse, Anwendungen und Technologien von der digitalen Bestellung von Waren und Dienstleistungen bis hin zur Fakturierung, elektronischen Bezahlung und Buchhaltung kennen.

a) Standards
   aa) Varianten des elektronischen Geschäftsverkehrs (D)

bb) Prinzipien und Technologien des Cloud Computing (V)
cc) Internetprotokolle (V)

b) Technologien
aa) Web Frameworks (ASP, Cocoon, JSF, Mason, Spring, Struts, Vaadin) (G)
bb) Dokumentenmanagement (Formen von Dokumenten, Technologien, Anwendungen) (G)

c) Prozesse und Anwendungen
aa) Online-Bestellsysteme (V)
bb) Online-Shops / Auktionsplattformen (D)
cc) Payment-Systeme (V)
dd) Warenwirtschaftssysteme (V)
ee) Finanzbuchhaltungssysteme (G)
ff) Lagerwirtschaft (G)
gg) CRM (G)
hh) Logistik / Versand (G)
ii) Suchmaschinenoptimierung (SEO) (V)

d) Social Media Marketing (V)
Lokalisierungsdienste

6.2.3. Enterprise Resource Planning (ERP)

Dieses Zusatzgebiet konzentriert sich auf die zahlreichen, komplexen und miteinander kommunizierenden Anwendungssystemen, die zur Unterstützung der Ressourcenplanung eines ganzen Unternehmens eingesetzt werden (ERP). Sachverständige müssen die grundsätzlichen fachlichen Prozesse der betroffenen Branchen kennen. Darüber hinaus müssen Sachverständige fundierte Kenntnisse von üblichen Lizenzmodellen, Schnittstellenanbindungen und Datenbanken sowie entsprechende Programmierkenntnisse besitzen.

a) Allgemeine Kenntnisse
aa) Einführungsstrategien für ERP-Systeme (D)
bb) Geschäftsprozessmodellierung (G)
cc) Mandantenfähigkeit (G)
dd) Customizing / Parametrisierung (V)
ee) E-Business (V)
ff) Lizenzmodelle (G)

b) Module eines ERP-Systems (V)
aa) Stammdatenverwaltung
bb) Finanzbuchhaltung
cc) Personalmanagement
dd) Waren-/ Materialwirtschaft/ Disposition
ee) Produktdatenmanagement
ff) Bedarfsermittlung
gg) Stücklistenmanagement
hh) CRM
ii) Vertrieb
jj) Auftragsabwicklung

kk) Produktionsplanung und -steuerung
ll) Rechnungswesen und Controlling
mm) Workflowsysteme
nn) Dokumentenmanagement
oo) Archivsysteme

6.2.4. IT-Forensik

Das Zusatzgebiet der IT-Forensik bettet die Sicherung, Analyse und Präsentation digitaler Spuren in den Rahmen der klassischen forensischen Wissenschaften ein. Dazu sind Kenntnisse im forensisch korrekten Vorgehen erforderlich. Gleichzeitig werden Informatikkenntnisse benötigt, um digitale Spuren und Daten verschiedenster Art und Abstraktionsebenen erfassen und forensisch korrekt bewerten zu können. Der Umgang mit forensischen Werkzeugen wird vorausgesetzt.

a) Allgemeine Kenntnisse
aa) Grundsätzliche Prinzipien der IT-Forensik (Grundlegende Definitionen, Chain of Custody, Nature of Evidence, Locard'sche Regel, Prozessmodelle) (D)
bb) Verwaltung von Asservaten (V)
cc) Kryptologie (Prinzipien, Verfahren, Anwendungen, Sicherheit) (V)
dd) Hashwerte (SHA1, ED2K, MD5) (V)
ee) Internet-Kommunikation (E-Mail, Chat, Messaging) (D)
ff) Bild- und Videoformate (JPEG, MPEG, EXIF) (D)
gg) Digitale Signaturen und Schlüsselverwaltungssysteme (V)
hh) Dateisysteme (FAT, NTFS, EXT2, EXT3, HFS, ReiserFS, EXT4, XFS, Lux) (V)
ii) Storage-Systeme (SATA, IDE, (I)SCSI, SAN, RAID 0-6, ReFS) und Datenträger (magnetische, optische Datenträger, Flashspeicher) (V)
jj) Virtualisierungssysteme (VMWare, Virtual PC, Citrix) (V)
kk) Cloudsysteme (Modelle, Strukturen, Zugriffs-, Sicherungs-, Analysemöglichkeiten) (V)
ll) Datentypen und Kodierungen (INTEGER, LONG, FLOAT, DOUBLE) (V)
mm) Netzwerk-Topologien (V)
nn) Netzwerkprotokolle (TCP/IP, DNS, DHCP, SMTP, POP, HTTP, SSL) (V)
oo) P2P-Systeme (Filesharing-Netzwerke und Client-Programme) (D)
pp) Internet-Browser (MS IE, Chrome, Safari, Opera, Mozilla) (D)
qq) Betriebssysteme (MS Windows, Linux, UNIX, iOS, Android, Mac OS, Symbian) (V)

b) Prozess und Vorgehensweise
aa) Planung von Sicherstellungsmaßnahmen (D)
bb) Schreibschutzmaßnahmen (D)
cc) Forensische Datensicherungsformate (V)
dd) Sicherung flüchtiger Datenbestände (RAM, Cold Boot) (V)
ee) Tools zur Datensicherung von mobilen Endgeräten und Rechnersystemen (D)
ff) Analyse verschlüsselter Daten (Rainbow-Tables, Brute Force, Dictionary) (D)
gg) Tools zur Auswertung (D)
hh) Anwendungsforensik (Artefakte aus Prefetch-, Cache-, History-, Cookie-, Bookmark-, Auslagerungs-Bereichen etc.) (D)
ii) Analyse unbekannter Anwendungen und deren Spuren (V)
jj) Timeline (Quellen, Konsolidierung, Analysen) (D)
kk) Auswertung von Konfigurationsdateien (Registry, INI-Files, .conf-Dateien) (D)
ll) Auswertung von Protokoll-Dateien (Event-Logs, Sys-Logs) (D)
mm) Rechtliche und Ethische Rahmenbedingungen (V)

nn) Datenschutz (V)
oo) Aufbereitung der Erkenntnisse (Inhalt, Darstellungsformen, Trennung von Tatsachen und Ableitungen) (D)
pp) Unterschiede bei der Beauftragung von Sachverständigen und bei der Art der Gutachtenerstattung im Zivilrecht und im Strafrecht, Abgrenzung zur Beauftragung als Ermittler (V)

c) Besondere rechtliche Kenntnisse (V)
aa) Wirtschaftsstraftaten, Betrug, Untreue, Rechtsstaat gefährdende Straftaten, Sexualstraftaten (unter anderem Kinderpornographie)
bb) Kenntnisse im Strafrecht und Strafprozessrecht (z. B. Verfahrensweisen im Ermittlungsverfahren, Auswertungsmöglichkeiten und Beweisverwertungsverbote)
cc) Urheberrechtsstraftaten, Thema Raubkopien, EDV-Strafrecht, Telekommunikationsgesetz und Überwachung der Telekommunikation
dd) Täterterminologie

6.2.5. IT-Sicherheit

Das Zusatzgebiet der IT-Sicherheit umfasst die Sicherheit von Informationen und Systemen, die am gesamten Zyklus der Informationsverarbeitung (Erfassung, Speicherung, Verarbeitung, Kommunikation, Löschung) beteiligt sind. Entsprechend sind Kenntnisse im Bereich der Sicherheitsgrundlagen erforderlich, welche in der Breite auf die IT-Einsatzgebiete übertragen und angewendet werden müssen.

a) Allgemeine Kenntnisse
aa) Schutzziele, Schwachstellen, Bedrohungen, Angriffe, rechtliche Rahmenbedin-gungen (D)
bb) IT-Forensik (G)
cc) Sicherheitsrichtlinien (IT-Sicherheitsgesetz), Sicherheitsinfrastruktur (V)

b) Spezielle Bedrohungen (V)
aa) Grundlagen, Angriffe, Gegenmaßnahmen zu relevanten Bedrohungen
bb) Malware (Viren, Würmer, Trojaner)
cc) Bot-Netze
dd) Spam, Phishing
ee) Denial-of-Service
ff) Mobiler Code, Mobile Apps

c) Netzwerk- und Internet-Sicherheit
aa) Kommunikationsgrundlagen (Klassen, Adressierungsarten, Topologien) (G)
bb) ISO/OSI-Referenzmodell, TCP/IP-Referenzmodell (Schichten, Protokolle, Dienste) (D)
cc) Firewall-Technologie (Paketfilter, DMZ, Proxy) (D)
dd) OSI-Sicherheitsarchitektur (V)
ee) Sichere Kommunikation (VPN, IPSec, SSL/TLS) (D)
ff) Sichere Anwendungsdienste (E-Mail, Zahlungsverkehr) (D)
gg) Web-Anwendungen (aktive Inhalte, Websockets, OWASP Top-Ten) (D)
hh) Mobile und drahtlose Kommunikation (GSM, UMTS, LTE, WLAN, Bluetooth, RFID, NFC) (D)
ii) Cloudsysteme (D)
jj) Analysewerkzeuge und Systemhärtung (Überwachung, IDS, IDP, Contentfilter) (D)

d) Betriebssystem-Sicherheit
   aa) Aufgaben, Arten und Aufbau von Betriebssystemen (D)
   bb) Administration, Rechtevergabe, Zugriffskontrolle (V)
   cc) Trusted Computing, Sicheres Booten (V)
   dd) Monitoring und Logging (V)
   ee) Analysewerkzeuge und Systemhärtung (D)

e) Kryptologie, Hashfunktionen, Signaturen
   aa) Grundlagen, Prinzipien, Methoden (V)
   bb) Informationstheorie (G)
   cc) Symmetrische, asymmetrische und hybride Verfahren (DES, Triple-DES, AES, RSA, ECC) (D)
   dd) Kryptografische Hashfunktionen (Grundlagen, Verfahren, MD5, SHA-x) (D)
   ee) Elektronische Signaturen (Verfahren, Standards, Signaturgesetz) (D)

f) Schlüsselmanagement, Authentifikation, Digitale Identität
   aa) Zertifizierung (Zertifikate, PKI) (D)
   bb) Schlüssel (Erzeugung, Aufbewahrung, Vernichtung, Austausch, Rückgewinnung) (D)
   cc) Authentifikation durch Wissen (Passwort-, Challenge-Response, Zero-Knowledge-Verfahren) (D)
   dd) Biometrie (Technik, Authentifikation) (D)
   ee) Authentifikation in verteilten Systemen (Radius, Kerberos) (D)
   ff) Smartcards (Architektur, Betriebssystem) (V)
   gg) Elektronische Identifikationsausweise (D)
   hh) Second Factor Authentifizierung (D)

g) Security Engineering, Bewertungskriterien, Sicherheitsmodelle
   aa) Entwicklungsprozess (V)
   bb) Strukturanalyse, Schutzbedarfsbestimmung, Bedrohungsanalyse, Risikoanalyse (V)
   cc) Sicherheitsarchitektur und Betrieb (V)
   dd) Security Development Lifecycle (V)
   ee) Bewertungskriterien (TCSEC, ITSEC, Common Criteria, Zertifizierungen) (V)
   ff) Sicherheitsmodelle (Klassifikation, Zugriffskontroll-, Informationsfluss-Modelle) (D)

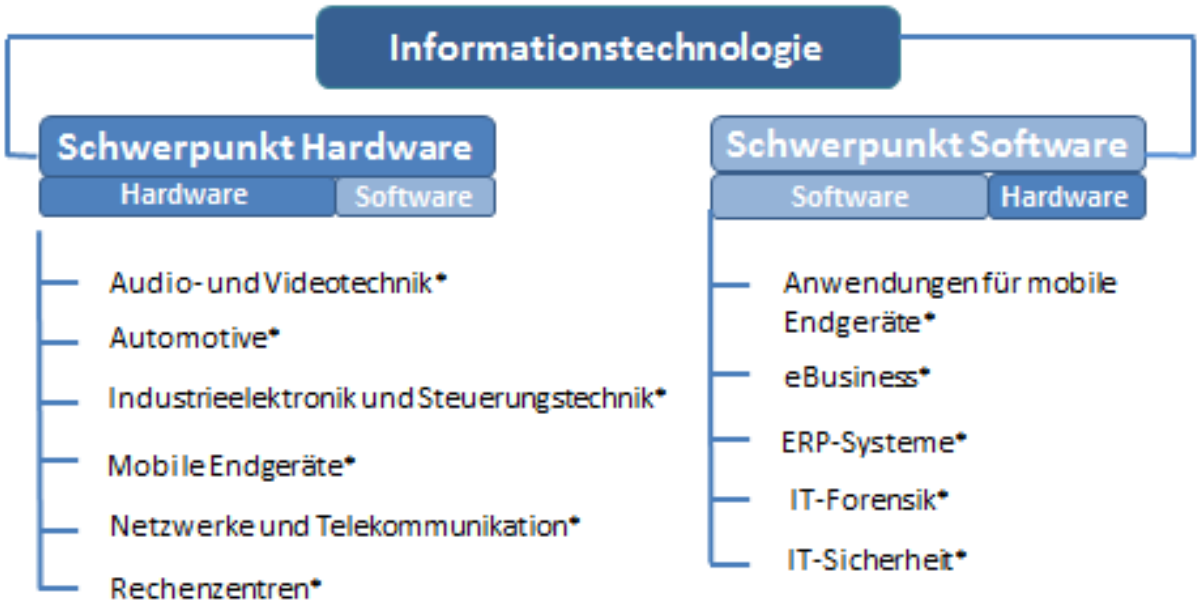
h) Datenschutz
   aa) Datenschutz (Recht, Umsetzung, Kontrolle) (D)
   bb) Governance (G)
   cc) Compliance (G)

7. Technische Ausstattung

Sachverständige müssen über eine angemessene EDV-Ausrüstung verfügen, die es ihnen erlaubt, Programme, Komponenten, Geräte und Rechner (auch im Verbund) zu prüfen. Sie müssen mit der Bedienung und den Funktionen der Systeme auf Hard- und Software-Ebene vertraut und in der Lage sein, Systeme selbst einzurichten. Sachverständige müssen mit dieser Ausrüstung Sachverhalte zuverlässig dokumentieren können.

Zusätzlich wird für den Schwerpunkt Hardware von den Sachverständigen erwartet, dass sie mit der Handhabung und Bedienung grundlegender Messgeräte vertraut sind und mindestens Zugriff auf, besser aber Eigenbesitz an diesen Geräten haben.

Anlage 1: Darstellung der Sachgebietseinteilung



* = Zusatzgebiet

Anlage 2:
Merkblatt zum Sachgebiet „IT – Schwerpunkt Software, insbesondere IT-Forensik“

Einleitung
Staatsanwaltschaften und Kriminalpolizei beauftragen vermehrt öffentlich bestellte und vereidigte IT-Sachverständige mit der Auswertung beschlagnahmter Hardware und Daten. Dabei geht es vor allem um die Aufklärung von Straftaten im Bereich der Wirtschaftskriminalität, strafbaren politischen Extremismus, Terrorismus sowie Kinderpornographie.

Besonderheiten bei der persönlichen Eignungsprüfung
Zusätzlich zur Prüfung der persönlichen Eignung durch die IHK erfolgt in einigen Bundesländern zusätzlich eine Sicherheitsüberprüfung durch die Staatsanwaltschaft oder Polizei. Davon können auch die Mitarbeiter der/des Sachverständigen betroffen sein. Die Sicherheitsüberprüfungen werden in regelmäßigen Abständen wiederholt. Darüber hinaus kann die Beauftragung in bestimmten Deliktsbereichen von einer vorgeschalteten speziellen Beschulung durch die Staatsanwaltschaft oder Polizei abhängig gemacht werden.

Räumliche Voraussetzungen
Die Überlassung inkriminierten Materials zu Auswertungszwecken wird in einigen Bundesländern in bestimmten Deliktsbereichen von der Erfüllung sicherheitstechnischer Voraussetzungen bei den Büroräumen abhängig gemacht. Hierbei sind gesteigerte Anforderungen an die Einbruchsicherheit zu stellen, wie auch an Vorkehrungen zur Verhinderung des unbefugten Zutritts während der Bürozeiten (Zugangskontrollen, intern gesicherte Bereiche) sowie an die Sicherung von Asservaten vor unberechtigtem Zugriff. Die Sicherheitsüberprüfung erfolgt durch die Staatsanwaltschaft oder Polizei und kann in regelmäßigen Abständen wiederholt werden.