2102

Informationstechnologie (IT)
Teilgebiet IT-Sicherheit

Sachgebietseinteilung
Fachliche Bestellungsvoraussetzungen

Stand: 06/2025
Revisionsnummer: 0
Erste Fassung: 06/2025

DIHK Deutsche Industrie- und Handelskammer
IfS

1 Sachgebietseinteilung und Bestellungstenor

Die Informationstechnologie (IT) hat alle Wirtschafts- und Lebensbereiche durchdrungen und besitzt eine wichtige Querschnittsfunktion.

Die Einteilung des interdisziplinären Sachgebiets beruht auf den Begrifflichkeiten eines durchschnittlichen IT-Anwenders, der Sachverständigenleistungen nachfragt. Die Inhalte sind breit gefasst und offen formuliert, um dem schnellen technischen Fortschritt gerecht zu werden und darzustellen, welche Sachverständige in einem spezifischen Anwendungsbereich Leistungen erbringen können. Dabei wurde eine herstellerunabhängige und produktneutrale Formulierung gewählt, auch um neue Entwicklungen auffangen zu können.

Die 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 alle IT-Einsatzgebiete übertragen und angewendet werden müssen.

Das Teilgebiet „IT-Sicherheit“ wurde geschaffen, um eigenständige Bestellungsvoraussetzungen für diesen Bereich zu schaffen. Es ist daher unabhängig von den Anforderungen für das Sachgebiet „Informationstechnologie“.

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

- IT-Sicherheit
- Informatik/Wirtschaftsinformatik
- Wirtschaftsinformatik
- Technische Informatik

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

oder

bei Antragstellenden ohne Hochschulabschluss der Nachweis von Erfahrung, Aus- und Fortbildung sowie regelmäßig eine 10-jährige praktische Tätigkeit, die ihrer Art nach geeignet sind, die erforderlichen Kenntnisse zu vermitteln.

2.2 In allen Fällen haben Antragstellende nachzuweisen, dass sie in fachverantwortlicher Stellung im Bereich der IT tätig sind und 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 sicherheitstechnische Betreuung von Systemen
- Erarbeitung umfangreicher IT-Sicherheitskonzepte und Dokumentationen
- Erarbeitung umfangreicher Leistungsspezifikationen im Bereich der IT-Sicherheit
- Erstellung von Gutachten oder vergleichbaren schriftlichen Ausarbeitungen.

2.3 Antragstellende sollen eine mindestens dreijährige einschlägige praktische Tätigkeit als Sachverständige/r im Gebiet IT-Sicherheit 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 fünf selbstverfassten Gutachten nachzuweisen. Die Gutachten sollen die Breites des Sachgebiets abdecken und sollen eine anspruchsvolle Fragestellung aufweisen.

Zum Aufbau eines Gutachtens wird auf die jeweilige Sachverständigenordnung sowie auf die „Hinweise zum Aufbau eines schriftlichen Sachverständigengutachtens” verwiesen.

3 Allgemeines

Antragstellende haben 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 6) in Klammern angegebenen Beispiele dienen lediglich zur Erläuterung. Sie erheben keinen Anspruch auf Vollständigkeit.

4 Allgemeine Kenntnisse

4.1 Rechtsgrundlagen

Die „Allgemeinen Rechtskenntnisse Sachverständigentätigkeit“ 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, 174, 176ff, 182, 184 a-d, 201 a, 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) (G)
f) Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) (V)
g) Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) (V)
h) Datenschutzgesetze (V)
i) Aktueller Stand der für den Bereich IT-Sicherheit relevanten Normen (NIS2, DORA, AI Act) (G)

5 Fachkenntnisse

Von den Sachverständigen wird erwartet, dass sie vor allem Störungs- und Ausfallmechanismen innerhalb des gesamten Spektrums ihres/seines Sachgebietes kennen und aufgrund ihres systematischen Fachwissens ermitteln und nachvollziehbar beschreiben und bewerten können.

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 Hardware

5.1.1 Baugruppen/Geräte (G)

a) Technologie, Aufbau und wesentliche Funktionen von Baugruppen und Geräten der Informationstechnologie
b) Rechner-/Steuereinheiten
c) Prozessoren (Typen, Aufbau, Kennwerte)
d) Sensoren und Sicherheitsmodule
e) Speichersysteme
f) Bus-Systeme
g) Schnittstellen
h) Montage, Verkabelung
i) Speicherprogrammierbare Steuerung (SPS)
j) Smarthome, IoT, Industrie 4.0 Komponenten
k) Peripherie
l) Massenspeicher (Festplatte, Band, CD, DVD, Halbleiter)
m) Eingabegeräte (Lesegeräte, Scanner, Sensoren)
n) Ausgabegeräte (Drucker, Displays)
o) Foto-, Video- und Audiogeräte

5.1.2 Systemarchitekturen (G)

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

5.1.3 Betrieb von Geräten, Anlagen und Rechenzentren (G)

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

5.2 Software

5.2.1 Informationstechnik (G)

a) Modellierung (Abstraktion, Graphen, Automaten, Strukturen, Prozesse, Berechenbarkeit)
b) Programmierparadigmen
c) Algorithmen und Datenstrukturen

5.2.2 Softwareengineering

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

o) Requirements Engineering (G)
p) Sichere Software- und Datenbankentwicklung (D)

5.2.3 Systemsoftware (V)

a) Betriebssysteme (allgemeine Grundlagen, Embedded, Real Time Operating Systems, MS Windows, Linux, UNIX, iOS, Android, Mac OS)
b) Microcode (Firmware), Assembler
c) Virtualisierungssysteme (allgemeine Grundlagen, VMware, Citrix, KVM)
d) Datenbankmanagementsysteme (DBMS) (Datenbankgrundlagen, Datenbankmodelle, Abfragesprachen, Transaktionsverwaltung, Datenintegrität, Data Warehouses)

5.2.4 Einsatz von Software

a) Standardsoftware (branchenübergreifende Lösungen, branchenspezifische Lösungen, ERP-Systeme, E-Commerce-Lösungen) (G)
b) Pflege und Wartung (Support-Organisation, Konfigurationsmanagement) (V)
c) Dokumentation (V)
d) Systemintegration und Betrieb von Schnittstellen (V)
e) Auswirkungen des IT- Einsatzes (Folgen, Risiken und Gefährdungspotentiale) (V)
f) Unternehmensübergreifende Software (CRM, SCM, EDI, EDIFACT) (G)
g) KI-Systeme (Sicherheit, KI-Systeme als Werkzeuge) (G)
h) Internet-Kommunikation (E-Mail, FTP, Chat, Messaging)
i) Industrielle-, IoT-, Smart-Home und Smart-City Anwendungen

5.2.5 Betrieb von Systemen

a) IT Service Management Best Practices (G)
b) Service Level Agreements (G)
c) Systemmonitoring (V)
d) Protokollierung und Logging (V)
e) Leistungs- und Abrechnungsformen (G)
f) Outsourcing und externer Datenspeicherung (organisatorisch, rechtlich) (V)
g) Konfigurationsmanagement (V)
h) Betrieb komplexer Systeme (V)

6 Spezialkenntnisse im Bereich IT-Sicherheit

6.1 Allgemeine Kenntnisse

a) Schutzziele, Schwachstellen, Bedrohungen, Angriffe, rechtliche Rahmenbedingungen (D)
b) Incident-Responce und IT-Forensik (V)
c) Sicherheitsrichtlinien, IT-Sicherheitsgesetze, Normen, Sicherheitsinfrastruktur (V)
d) Governance (G)
e) Compliance (G)
f) Offensive IT-Sicherheit (PEN-Testing, Red- und Blue-Teaming) (V)
g) Human Factors in der IT-Sicherheit (Awareness-Training) (G)
h) IT-Sicherheitsmanagement

6.2 Spezielle Bedrohungen (V)

a) Grundlagen, Angriffe, Gegenmaßnahmen zu relevanten Bedrohungen
b) Malware (Viren, Würmer, Trojaner)
c) Bot-Netze
d) Spam, Phishing
e) Denial-of-Service
f) Mobiler Code, Mobile Apps
g) Social Engineering
h) Hardwarenahe Angriffe

6.3 Netzwerk- und Internet-Sicherheit

a) Kommunikationsgrundlagen (Klassen, Adressierungsarten, Topologien) (V)
b) ISO/OSI-Referenzmodell, TCP/IP-Referenzmodell (Schichten, Protokolle, Dienste) (D)
c) Firewall-Technologie (Paketfilter, DMZ, Proxy, NextGeneration) (D)
d) OSI-Sicherheitsarchitektur (V)
e) Sichere Kommunikation (VPN, IPSec, SSL/TLS) (D)
f) Sichere Anwendungsdienste (E-Mail, Zahlungsverkehr) (D)
g) Web-Anwendungen (aktive Inhalte, Websockets, OWASP Top-Ten) (D)
h) Mobile und drahtlose Kommunikation (GSM, LTE, WLAN, Bluetooth, RFID, NFC) (D)
i) Cloudsyteme (D)
j) Analysewerkzeuge und Systemhärtung (Überwachung, IDS, IDP, SIEM, UTM, Contentfil-ter) (D)

6.4 Betriebssystem-Sicherheit (V)

a) Administration, Rechtevergabe, Zugriffskontrolle
b) Trusted Computing, Sicheres Booten
c) Monitoring und Logging
d) Analysewerkzeuge und Systemhärtung

6.5 Kryptologie, Hashfunktionen, Signaturen

a) Grundlagen, Prinzipien, Methoden (D)
b) Informationstheorie (G)
c) Symmetrische, asymmetrische und hybride Verfahren (DES, Triple-DES, AES, RSA, ECC) (V)
d) Kryptografische Hashfunktionen (Grundlagen, Verfahren, MD5, SHA-x) (V)
e) Elektronische Signaturen (Verfahren, Standards, eIDAS VO) (V)

6.6 Schlüsselmanagement, Authentifikation, Digitale Identität

a) Zertifizierung (Zertifikate, PKI) (D)
b) Schlüssel (Erzeugung, Aufbewahrung, Vernichtung, Austausch, Rückgewinnung) (D)
c) Authentifikation durch Wissen (Passwort-, Challenge-Response, Zero-Knowledge-Verfahren) (D)
d) Biometrie (Grundlagen, Technik, Authentifikation) (D)
e) Authentifikation in verteilten Systemen (Radius, Kerberos) (D)
f) Smartcards (Architektur, Betriebssystem) (V)
g) Elektronische Identifikationsausweise (D)
h) Multi-Faktor-Authentifizierung (D)

6.7 Security Engineering, Bewertungskriterien, Sicherheitsmodelle (V)

a) Entwicklungsprozess
b) Strukturanalyse, Schutzbedarfsbestimmung, Bedrohungsanalyse, Risikoanalyse
c) Sicherheitsarchitektur und Betrieb
d) Security Development lifecycle
e) Bewertungskriterien (TCSEC, ITSEC, Common Criteria, Zertifizierungen)
f) Sicherheitsmodelle (Klassifikation, Zugriffskontroll-, Informationsfluss-Modelle)

7 Technische Ausstattung

Sachverständige müssen über eine angemessene IT-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.