

Berliner Feuerwehr	Stand: Mai 2025
Anforderungsprofil Leitende Sachbearbeitung im Sachgebiet technische Informationssicherheit im Hauptsachgebiet IKT-Sicherheit	Stellenzeichen ES IKT Sich 22

A	<p>1. Beschreibung des Arbeitsgebietes: (Aufgabenbeschreibung)</p> <p>1. Leitende Sachbearbeitung im Sachgebiet technische Informationssicherheit im Hauptsachgebiet IKT-Sicherheit</p> <ul style="list-style-type: none"> • Unterstützung der Sachgebietsleitung bei der Planung, Koordination und Überwachung von Personal- und Arbeitseinsatz des zugeordneten Sachgebietes • Überwachung und Incident-Behandlung der Sicherheitssysteme in Zusammenarbeit mit dem IT-Betrieb. Die Erfassung von Sicherheitsvorfällen erfolgt durch Meldungen von anderen Bereichen, automatischen Meldungen, Monitoring von Systemen und perspektivisch über ein zentrales Logging und Monitoring System. Die Behandlung erfolgt individuell und problembezogen, in Abstimmung mit den betroffenen Bereichen • Weiterentwicklung und Anpassung der technischen Sicherheitsarchitektur des Berliner Feuerwehr Daten-Netzes (BFDN), durch Arbeit an Vorgaben und Richtlinien, Kommunikation mit den Fachbereichen und Prüfung der Umsetzung • Sicherstellung einer aktuellen Schwachstellen- und Risikobewertung für die Berliner Feuerwehr auf Grundlage von externen CERT-Informationen inklusive der zu erstellenden Berichterstattung. Dies umfasst die Sichtung von CERT Meldungen, die Prüfung der Betroffenheit der Feuerwehr (bei Bedarf in Rücksprache mit den entsprechenden Fachbereichen) und die Einordnung des Ausmaßes und der Schwere der Betroffenheit für die Berliner Feuerwehr • Stellvertretende Wahrnehmung von Gremientätigkeit im Umfeld der Cybersicherheit, bspw. Vertretung der Berliner Feuerwehr beim Cybersicherheitsgremium „CyBerlin“ der Senatsverwaltung für Inneres und Sport • Mitglied eines internen Cyber-Response Team der Berliner Feuerwehr • Erarbeitung von technischen Sicherheitsrichtlinien der zentralen Sicherheitssysteme, d.h. Vorgaben zur Installation und Betrieb von Komponenten/Software wie bspw. Firewalls • Erstellung von datenschutzkonformem Betrieb,- und Auswertungskonzepten für ein SIEM-System • Federführende Unterstützung bei der Planung und Koordinierung der durchzuführenden Arbeiten im Sachgebiet, wie z.B. Abarbeitung von Tickets, einschließlich der Terminüberwachungen und der Ergebniskontrollen • Anleitung, Beratung und Förderung der zugeordneten Mitarbeitenden zur Sicherstellung der durch den Sachgebietsleiter festgelegten Sachgebietsziele und somit gezielte Einflussnahme auf deren fachliche und empathische Weiterentwicklung • Enge Zusammenarbeit mit den Führungskräften aller Organisationseinheiten der Berliner Feuerwehr, beispielsweise unterstützend bei der Einführung von neuen Sicherheitsrichtlinien oder bei der Behandlung von Sicherheitsvorfällen • Stellv. Leitung des Sachgebietes technische Informationssicherheit
----------	---

2. Einbindung in die Sicherheitsüberwachungssysteme

- Unterstützung eines SIEM-Projektes mit dem Ziel die Informationen unterschiedlicher Sicherheitssysteme (z.B. Mailgateway, Firewall, Endpoint, NAC, ...) zu einem ganzheitlichen Cybersicherheitslagebild der Behörde zu verdichten. Dies umfasst Mitarbeit bei Auswahl und Aufbereitung der zu verarbeitenden Informationen, sowie beim Erstellen und Bearbeiten von Sicherheitsmeldungen

- Beratung und Unterstützung der Abteilungen und des IKT-Betriebsbereiches bei Integration von Basisdiensten und Fachdiensten in das Security-Monitoring

- Etablierung und nachfolgend Gewährleistung der Erstellung ganzheitlicher automatisierter Überwachungsberichte

Federführende Bearbeitung von komplexen Security-Events in Zusammenarbeit mit dem IT-Betrieb, zum Beispiel bei gezielten Angriffen, oder Ausfällen von Systemen. Dies umfasst eine Einordnung • der Vorfälle, Ermittlung von beteiligten Akteuren, und laufende Kommunikation mit Stakeholdern

- Etablierung eines regelhaften Security-Incident Prozesses und Integration in bestehende ITIL-Prozesse bei der Berliner Feuerwehr

- Abstimmung von Regelungen und organisatorischen Festlegungen mit dem Bereich Notfallmanagement der Berliner Feuerwehr

3. Forensik

- Unterstützung bei der Erstellung und Pflege einer Forensik-Richtlinie, die beschreibt, wie nach einem Vorfall Daten gesichert, analysiert und aufbereitet werden

- Identifizierung und Vergabe von externen Dienstleistungen im Forensik-Umfeld, d.h. Beauftragung von externen professionellen IT-Forensik Dienstleistern, insofern interne Kompetenzen für Vorfallbehandlungen nicht ausreichend gegeben sind

- Durchführung von sensitiven datenschutzrelevanten Eingriffen und Auswertungen im Bereich Sicherheitssysteme und Forensik, wie z.B. das Auslesen und Auswerten von Datenträgern und Datenverbindungen zur Rekonstruktion und Aufarbeitung von Vorfällen

- Konzeptionierung und prototypische Installation einer isolierten und abgesicherten internen Infrastruktur zur Durchführung von Sicherheitsuntersuchungen, z.B. für Internet of Things Geräte, externe Datenträger, Apps usw.

Führungsebene: keine

Besonderheiten:

Stellenbewertung: E12 Teil II TV-L

B	Anforderungen
1.	Formale Anforderungen (bitte entsprechend ergänzen)
	<ul style="list-style-type: none"> • abgeschlossene Hochschulausbildung (Bachelor- bzw. vergleichbarer Hochschulabschluss) im Bereich Informatik, Informationstechnik oder vergleichbar oder • abgeschlossene Hochschulausbildung (Bachelor- bzw. vergleichbarer Hochschulabschluss) in verwandten MINT-Richtungen oder • einschlägige abgeschlossene Berufsausbildung und entsprechende mehrjährige Tätigkeit von mindestens 3 Jahren im geforderten IT-Bereich oder •
2.	ggf. gesundheitliche Anforderungen (bitte entsprechend ergänzen)
	<p><input checked="" type="checkbox"/> fachliche Anforderungen:</p> <p>Für zur Bewältigung des Aufgabenkreises erforderliche Erfahrungen usw.</p> <ul style="list-style-type: none"> • Mindestens dreijährige Berufserfahrung im Bereich IT-Betrieb, speziell im Bereich IT-Netzwerke oder Systemadministration • Erfahrungen über Routing und Aufbau IP basierter Netze • Erfahrungen mit IT-Betriebsprozessen z.B. nach ITIL v4 oder COBIT • Erfahrungen über den Betrieb von IT-Sicherheitskomponenten wie z.B. Firewalls • Fachspezifische Englischkenntnisse sind erforderlich <p>Wünschenswert:</p> <ul style="list-style-type: none"> • Kenntnisse im Bereich Prävention, Detektion oder Analysemöglichkeiten von Angriffen • Erweiterte Kenntnisse zu technischen Merkmalen aber auch Gegenmaßnahmen zu staatlich gelenkten aber auch kommerziellen Cyberattacken • Kenntnisse zu technischen Richtlinien und Vorgaben vom BSI • Kenntnisse von Cybersecurity Frameworks und Normen (z.B. MITRE ATT&CK, MITRE D3FEND, NIST Cybersecurity Framework, Cyber Kill Chain)

3. Erläuterungen zur Gewichtung und Prioritätenvergabe:

Gewichtungen:

Die Gewichtungen drücken aus, welche Bedeutung die einzelnen Kompetenzen, bezogen auf das Aufgabengebiet, haben, welche Relevanz ihnen zukommt, um die übertragenen Aufgaben erfolgreich ausführen

zu können. Insgesamt gilt, dass die gesamte vierstufige Skalierung zu nutzen ist. Nicht jede Kompetenz kann und muss in besonders ausgeprägter Form vorliegen. In Führungspositionen nehmen die außerfachlichen Anforderungen im Verhältnis zu den fachlichen Anforderungen zu. Eine Gewichtung der

Stufe 1 „wünschenswert“ findet daher in den Profilen für Führungspositionen eher im Bereich der fachlichen Anforderungen Anwendung. Auch der prozentuale Anteil am gesamten Aufgabengebiet ist ggf. ein Indiz für die Gewichtung.

Gewichtungen:

- 4 unabdingbar
- 3 sehr wichtig
- 2 wichtig
- 1 wünschenswert

Prioritäten:

Diese Einschätzung soll nur bei Auswahlverfahren als Hilfestellung dienen.

Bei der Prioritätenvergabe wird zusätzlich zur Gewichtung festgehalten, welche der geforderten Fähigkeiten

I: mittelfristig
II: kurzfristig
III: sofort

vorhanden sein müssen.

						bei Auswahlverfahren
		Gewichtungen				Priorität
		4	3	2	1	III / II / I
3.1 Fachkompetenzen						
3.1.1	<ul style="list-style-type: none"> Erweiterte Kenntnisse im Bereich IT-Netzwerke und Systemadministration 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	III
3.1.2	<ul style="list-style-type: none"> Erweiterte Kenntnisse über Methodik, Gefährdungen und Angriffspraktiken im Bereich Cybersicherheit, sowie der Prävention, Detektion und Analysemöglichkeiten von entsprechenden Angriffen 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	III
3.1.3	<ul style="list-style-type: none"> Erweiterte Kenntnisse zu Cybersicherheitsarchitekturen, technischer Detektion und Reaktion sowie die Fähigkeit in unterschiedlichen technischen Abstraktionsebenen zu kommunizieren 	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	I
3.1.4	<ul style="list-style-type: none"> Erweiterte Kenntnisse von Client/Server Infrastrukturen, OSI-Modell (Open Systems Interconnection model), TCP/IP (Transmission Control Protocol/Internet Protocol) und Standard-Netzwerkprotokollen 	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	I
3.1.5	<ul style="list-style-type: none"> Kenntnisse des Datenschutzes im Umfeld von Sicherheitssystemen, z.B. Kenntnis vom Standard-Datenschutzmodell (SDM) 	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	I
3.1.6	<ul style="list-style-type: none"> Kenntnisse der Rahmenbedingungen der IKT-Sicherheit und des CERT im Bund und im Land Berlin 	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	II
3.1.7	<ul style="list-style-type: none"> Kenntnisse wichtiger technischer und politischer Akteure im Bereich Cybersicherheit in Deutschland und speziell in Berlin, wie z.B. das Bundesamt für Sicherheit in der Informationstechnik (BSI), das IT-Dienstleistungszentrum Berlin (ITDZ Berlin) oder die Senatsverwaltung für Inneres und Sport 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	II
3.1.8	<ul style="list-style-type: none"> Kenntnisse über Organisation, Aufbau und Personalstruktur der Berliner Feuerwehr, Freiwilligen Feuerwehr sowie anderer relevanter Behörden 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	I
3.1.9	<ul style="list-style-type: none"> Kenntnisse rechtlicher Grundlagen, insbesondere bei personalrechtlichen Angelegenheiten von Beamten und Beamtinnen sowie Beschäftigten (LBG, BeamtStG, TV-L, GGO I, DA, GA, KGSt) sowie fundierte Kenntnisse zum Datenschutz und zur Datensicherung) sowie IKT-Sicherheitsrichtlinien (GA, DV, BlnDSG, DSGVO, BDSG) 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	I
3.2.1	<ul style="list-style-type: none"> Grundlegende Kenntnisse der von ES IKT betriebenen IKT-Infrastrukturen und IKT-Dienste, sowie maßgeblicher IKT-Systeme von Dritten, bspw. dem ITDZ Berlin 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	I
3.2.2	<ul style="list-style-type: none"> Kenntnisse über das Zusammenwirken der IKT-Systeme, den Auswirkungen von Ausfällen durch Cybergefährdungen, der Wiederherstellung der IKT-Systeme und Mitigation 	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	II

						bei Auswahlverfahren
		Gewichtungen				Priorität
		4	3	2	1	III / II / I
3.2.3	<ul style="list-style-type: none"> • Kenntnisse im Bereich Schwachstellenmanagement (Schwachstellenscans, Bewertung von Schwachstellen, Maßnahmen) 	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	II
3.2.4	<ul style="list-style-type: none"> • Kenntnisse zur Nachbereitung von Sicherheitsvorfällen 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	I
3.2.5	<ul style="list-style-type: none"> • Kenntnis von Relevanten Gesetzen, Normen und Richtlinien im Bereich IT-Sicherheit (§ 23 EGovG Bln, BSI 200-1, BSI 200-2, BSI 200-3, BSI 200-4, ISO 27001, ISO 27005, NIST Standards, DSGVO, SDM, ITIL v4, COBIT) 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	I
3.2.6	<ul style="list-style-type: none"> • Fachspezifische Englischkenntnisse 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	III
3.3 Persönliche Kompetenzen						
3.3.1	<p>Leistungs-, Lern- und Veränderungsfähigkeit</p> <ul style="list-style-type: none"> ▶ Fähigkeit, auch unter schwierigen Bedingungen engagiert zu arbeiten, den Handlungsrahmen auszufüllen und aktiv Wissen und Erfahrungen einzubringen sowie sich auf neue Aufgaben einzustellen und neue Kenntnisse zu erwerben. ▶ arbeitet ohne nennenswerte Fehler und Leistungsschwankungen ▶ bewältigt seine Aufgaben bei gleichbleibend guter Qualität ▶ geht aktiv und engagiert an Aufgaben heran ▶ bewältigt das vorgegebene Arbeitspensum ▶ bringt eigene Informationen zum Nutzen aller Beteiligten ein ▶ stellt sich veränderten Anforderungen im Aufgabengebiet ▶ erkennt eigenen Fortbildungsbedarf und wird initiativ tätig bildet sich anforderungsgerecht fort 	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	III
3.3.2	<p>Organisationsfähigkeit</p> <ul style="list-style-type: none"> ▶ Fähigkeit, vorausschauend zu planen und zu strukturieren und entsprechend zu agieren. ▶ koordiniert Arbeitsabläufe sach-, zeit- und personengerecht ▶ arbeitet vorausschauend ▶ koordiniert eigene Termine und stimmt diese rechtzeitig ab ▶ richtet die Arbeitsorganisation auf die zu erreichenden Ziele aus 	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	II

						bei Auswahlverfah- ren
		Gewichtungen				Priorität
		4	3	2	1	III / II / I
3.3.3	Ziel- und Ergebnisorientierung ► Fähigkeit, Denken und Handeln auf ein gewünschtes Ziel hin auszurichten und die erforderlichen Ressourcen effizient einzusetzen.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	II
3.3.4	Entscheidungsfähigkeit ► Fähigkeit, zeitnahe und nachvollziehbare Entscheidungen zu treffen und dafür Verantwortung zu übernehmen. ► setzt in Eigeninitiative die für seine Funktion notwendigen Schwerpunkte und handelt danach ► setzt sich engagiert für selbst oder von außen gesetztem Ziel ein ► arbeitet mit geringer Anleitungserfordernis ► greift Probleme aus eigenem Antrieb auf ► beschafft sich weitgehend selbständig notwendige Informationen ► gibt bei Widerständen nicht gleich auf handelt zielorientiert	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	I
3.3.5	Belastbarkeit ► behält bei hohem Arbeitsanfall, schwierigen Entscheidungslagen und in belastenden Situationen den Überblick und reagiert angemessen ► arbeitet qualitativ zufriedenstellend auch bei Belastungsspitzen ► übernimmt bereitwillig neue Aufgaben ► resigniert nicht bei Rückschlägen ► bewältigt wechselnde Arbeitsinhalte und -situationen ► bleibt auch unter Leistungsdruck besonnen und sachlich	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	II
3.4 Sozialkompetenzen						
3.4.1	Kommunikationsfähigkeit ► Fähigkeit, sich personen- und situationsbezogen auszutauschen. ► hält Kommunikationsregeln ein und zeigt Interesse am Gegenüber ► stellt klärende Fragen und lässt Nachfragen zu ► holt Informationen ein und gibt Informationen in alle Ebenen und zuständigen Bereiche weiter ► baut Kontakte/Netzwerke auf und pflegt sie ► gibt Informationen aktuell, umfassend, gezielt und verständlich weiter argumentiert und handelt situations- und personenbezogen	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	III

						bei Auswahlverfahren
		Gewichtungen				Priorität
		4	3	2	1	III / II / I
3.4.2	Kooperationsfähigkeit ► Fähigkeit, sich konstruktiv respektvoll mit anderen auseinanderzusetzen und partnerschaftlich zusammenzuarbeiten; Konflikte zu erkennen und tragfähige Lösungen anzustreben. ► arbeitet konstruktiv und vertrauensvoll mit anderen zusammen ► vertritt nicht zu beeinflussende Vorgaben loyal ► verhält sich kollegial und hilfsbereit ► zeigt anderen eine positive Einstellung hat Verständnis für Stärken und Schwächen anderer	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	III
3.4.3	Konflikt- und Kritikfähigkeit ► erkennt, wo und wodurch Konflikte entstehen und strebt mit den Beteiligten eine Konsenslösung an ► bleibt in Konfliktsituationen sachlich und ausgeglichen ► bleibt als nicht direkt Beteiligter unparteiisch ► lässt Kritik an eigener Person oder eigenem Verhalten zu ► reflektiert die eigene Arbeit und das Verhalten kritisch und ändert es gegebenenfalls ► kritisiert sachlich ohne zu verletzen	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	II
3.4.4	Dienstleistungsorientierung ► Fähigkeit, die Arbeit als Dienstleistung für externe und interne Kund*innen zu begreifen. ► begreift seine Aufgabe als Dienst- und Serviceleistung ► verhält sich im Kundenkontakt freundlich, aufgeschlossen und verbindlich ► berücksichtigt die Sichtweise und Bedürfnisse seines Gegenübers ► handelt situationsgerecht und hält Zusagen ein ► gestaltet sein Äußeres der Aufgabe und Situation entsprechend ist sich kultureller, religiöser und geschlechtlicher Unterschiede bewusst und berücksichtigt diese bei der Aufgabenerfüllung	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	II
3.4.5	Diversity-Kompetenz ► Fähigkeit, Gemeinsamkeiten und Unterschiede von Menschen (u. a. hinsichtlich Lebensalter, Geschlecht, Behinderung, Migrationsgeschichte, Religion, sexueller und geschlechtlicher Identität, chronischer Krankheit, sozialem Status, Sprache) wahrzunehmen, in der Aufgabenwahrnehmung zu berücksichtigen, bestehende Barrieren abzubauen und einen diskriminierungsfreien und wertschätzenden Umgang zu pflegen.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	I

						bei Auswahlverfah- ren
		Gewichtungen				Priorität
		4	3	2	1	III / II / I
3.4.6	<p>Migrationsgesellschaftliche Kompetenz</p> <p>► umfasst die Fähigkeit gemäß § 3 Abs. 4 PartMigG</p> <ol style="list-style-type: none"> 1. bei Vorhaben, Maßnahmen und Programmen die Auswirkungen auf Personen mit und ohne Migrationsgeschichte beurteilen und ihre Belange berücksichtigen zu können, 2. die durch Diskriminierung und Ausgrenzung von Personen mit Migrationsgeschichte entstehenden teilhabehemmenden Auswirkungen zu erkennen und zu überwinden sowie 3. insbesondere im beruflichen Kontext Personen mit Migrationsgeschichte respektvoll und frei von Vorurteilen und Diskriminierung zu behandeln. 	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	II

