



Remote - IT Security Berater (m/w/d)

Für unseren Kunden suchen wir einen "IT-Security-Berater" (m/w/d).

Rahmenparameter

- + **Start:** asap
- + **Laufzeit:** asap bis 28.02.2027 (ca. 5 Monate)
- + **Auslastung:** Teilauslastung – Gesamtumfang von 20 Personentagen, flexibel über die Projektlaufzeit verteilt (+/- 10 % möglich)
- + **Einsatzort:** Remote

Projektbeschreibung

Unser Kunde, ein Auftraggeber aus dem öffentlichen Sektor, betreibt eine umfangreiche Rechenzentrumsinfrastruktur mit zentralen Hardware- und Softwarekomponenten sowie bestehenden Wartungs-, Support- und Beschaffungsbeziehungen zu Herstellern und Dienstleistern. Da die bestehenden Sicherheitslösungen bzw. deren Wartungs- und Supportverträge mittelfristig auslaufen, gleichzeitig aber die IT-Sicherheit der vorhandenen Systeme durchgängig sichergestellt werden muss, soll im Rahmen dieses Einzelabrufs eine GAP-Analyse der technischen IT-Sicherheit durchgeführt werden.

Ziel des Projekts ist die Aufnahme und Bewertung der für die IT-Sicherheit relevanten Hardware- und Softwarelandschaft sowie die Ableitung prioritärer Handlungsoptionen für die künftige Betriebs- und Beschaffungsstrategie. Die Analyse konzentriert sich dabei nicht auf eine vollständige Detailbetrachtung, sondern priorisiert nach IT-Sicherheitsrelevanz – insbesondere auf technische Sicherheitslösungen, über Sicherheitsarchitekturen sowie sicherheitsrelevante Funktionen geschäftskritischer Plattformen und Anwendungen. Nichttechnische Themen wie Awareness, Governance, Richtlinien oder Prozessdokumentation sind ausdrücklich nicht Gegenstand der Betrachtung.

Aufgaben

- + Aufnahme und Bewertung der für die IT-Sicherheit relevanten Hardware- und Softwarelandschaft des Auftraggebers, unter vorrangiger Berücksichtigung bereits vorhandener Informationen
- + Vertiefte Analyse technischer Sicherheitslösungen, übergreifender Sicherheitsarchitekturen sowie sicherheitsrelevanter Funktionen geschäftskritischer Plattformen und Anwendungen
- + Bewertung bestehender Wartungs-, Support- und Beschaffungsabhängigkeiten, insbesondere im Hinblick auf auslaufende Verträge und Ersatzbeschaffungen
- + Identifikation und Darstellung bestehender technischer Sicherheitslücken sowie Ableitung wirtschaftlich und technisch umsetzbarer Lückenschließungsoptionen (Optimierung bestehender Lösungen, Upgrades, zusätzliche Sicherheitskomponenten)
- + Berücksichtigung und Überführung relevanter Anforderungen aus BSI-Gesetz (BSIG), BSI IT-Grundschutz, branchenspezifischem Sicherheitsstandard (B3S) und NIS2 in technische Soll-Anforderungen sowie Abgleich mit dem vorhandenen Sicherheitsniveau (keine Compliance-, Governance- oder ISMS-Prüfung)
- + Erstellung geeigneter Visualisierungen der Sicherheitsabdeckung, bestehender Lücken, Abhängigkeiten sowie möglicher Veränderungen und Optimierungsmaßnahmen (inkl. Vertragslaufzeiten, Ersatzbeschaffungen, Plattformentscheidungen, Ablöszenarien)
- + Einordnung, inwieweit bestehende oder künftige Rahmenverträge für die strategischen Zielbilder der IT-Sicherheit geeignet sind; ergo Betrachtung weiterer Beschaffungswege soweit entscheidungsrelevant
- + Erarbeitung einer priorisierten IT-Sicherheits-Roadmap mit kurz-, mittel- und langfristigen Handlungsfeldern inkl. erwartetem Beitrag zur Betriebssicherheit, IT-Sicherheitsniveau, Wirtschaftlichkeit und Risikoreduzierung
- + Erstellung kompakter, entscheidungsfähiger Unterlagen zur Entscheidungsvorbereitung im zuständigen Führungskreis des Auftraggebers

- + Durchführung notwendiger Ist-Aufnahmen, Interviews, Workshops und Bedarfsabfragen in eng begrenztem, für die Arbeitsergebnisse erforderlichem Umfang, um den laufenden Betrieb des Auftraggebers nicht unverhältnismäßig zu belasten

Erfahrungen & Kenntnisse

- + Mehrjährige Erfahrung in der Bewertung komplexer IT-Infrastrukturen und der IT-Sicherheit, idealerweise mit Bezug zu öffentlichen Auftraggebern
 - + Expertenwissen zu Rechenzentrumsinfrastrukturen, insbesondere Server, Storage, Virtualisierung, Betriebssysteme, Datenbanken und systemnaher Software
 - + Fundierte Kenntnisse in Sicherheitsarchitekturen, technischer Bestandsbewertung und Schwachstellenmanagement
 - + Erfahrung mit Cloud- und Hybrid-Cloud-Szenarien
 - + Expertenwissen in der Bewertung von Betriebsrisiken, technischen Abhängigkeiten, Wirtschaftlichkeit sowie in der Priorisierung von Handlungsoptionen
 - + Fundierte Kenntnisse der regulatorischen Rahmenbedingungen: BSI-Gesetz (BSIG), BSI IT-Grundschutz, branchenspezifischer Sicherheitsstandard (B3S) sowie NIS2
 - + Erfahrung in der Erstellung von Entscheidungsunterlagen und Visualisierungen für Führungsgremien öffentlicher Auftraggeber
 - + Wünschenswert: Kenntnisse zu Beschaffungswegen des öffentlichen Sektors, eigenverantwortliche, selbstorganisierte Arbeitsweise sowie Deutschkenntnisse (für Abstimmung mit dem Führungskreis)
-