STELLENBESCHREIBUNG

IT-Systemadministrator (m/w/d)
Schwerpunkt IT-Security, Firewall, Windows Server & Microsoft 365

I. Stellenbezeichnung
IT-Systemadministrator (m/w/d)

II. Ziel der Stelle
Der IT-Systemadministrator gewährleistet den sicheren, stabilen und wirtschaftlichen Betrieb der gesamten IT-Infrastruktur des Unternehmens. Der Schwerpunkt liegt auf der Informationssicherheit, der Administration von Microsoft-Umgebungen, der Netzwerk- und Firewall-Sicherheit sowie der kontinuierlichen Dokumentation und Optimierung der IT-Landschaft.
Darüber hinaus unterstützt die Position die Umsetzung von IT-Sicherheitsstandards, Compliance-Anforderungen sowie die Weiterentwicklung der Unternehmens-IT. Die Grundlage bilden die Aufgaben aus der bestehenden Stellenbeschreibung, insbesondere Netzwerksicherheit, Datensicherheit, Systembetreuung, Monitoring und Dokumentation.

III. Organisatorische Einordnung
Berichtet an den IT-Leiter. Enge Zusammenarbeit mit Fachbereichen, Management, Kunden, Auditoren und externen Dienstleistern.

Berichtslinie
- Direkte Berichtslinie an den IT-Leiter
- Enge Zusammenarbeit mit Fachbereichen, externen Dienstleistern und Softwareanbietern

Stellvertretung
- Vertretung anderer IT-Mitarbeiter im Rahmen der fachlichen Aufgaben
- Übernahme definierter IT-Verantwortlichkeiten bei Abwesenheit des IT-Leiters

IV. Hauptaufgaben und Verantwortlichkeiten

1. IT-Security und Informationssicherheit
- Umsetzung und Weiterentwicklung der IT-Sicherheitsstrategie
- Überwachung und Absicherung der Unternehmensnetzwerke
- Administration und Konfiguration von Firewalls, VPN-Lösungen und Netzwerksicherheitskomponenten
- Durchführung von Sicherheitsanalysen und Schwachstellenbewertungen
- Bearbeitung und Nachverfolgung von Security Incidents
- Einführung und Überwachung von Sicherheitsrichtlinien
- Verwaltung von Benutzer-, Rollen- und Berechtigungskonzepten
- Unterstützung von Audits sowie Einhaltung von ISMS-, TISAX-, ISO 27001- oder vergleichbaren Anforderungen

- Umsetzung von Multi-Faktor-Authentifizierung (MFA), Conditional Access und Zero-Trust-Konzepten
- Planung und Durchführung von Security-Awareness-Maßnahmen

2. Firewall- und Netzwerkadministration

- Administration und Überwachung der Firewall-Infrastruktur
- Einrichtung und Pflege von VPN-Verbindungen zwischen Standorten, Kunden und Geschäftspartnern
- Verwaltung von Switches, Routern, WLAN-Systemen und Netzwerksegmentierungen
- Überwachung der Netzwerkperformance und Verfügbarkeit
- Analyse und Behebung von Netzwerkstörungen
- Durchführung von Firmware- und Security-Updates
- Pflege der Netzwerkdokumentation einschließlich Topologien und Regelwerken

3. Windows Server Administration

- Installation, Konfiguration und Administration von Windows-Server-Systemen
- Verwaltung von Active Directory, Gruppenrichtlinien (GPO) und DNS/DHCP
- Administration von File- und Print-Services
- Betrieb und Weiterentwicklung virtueller Serverumgebungen
- Planung und Umsetzung von Server-Migrationen und System-Upgrades
- Performance- und Kapazitätsmanagement
- Sicherstellung hoher Verfügbarkeit und Systemstabilität

4. Microsoft 365 Administration

- Administration der Microsoft 365 Umgebung
- Verwaltung von Exchange Online, Teams, SharePoint Online und OneDrive
- Benutzer- und Lizenzmanagement
- Verwaltung von Microsoft Entra ID (Azure AD)
- Implementierung und Betreuung von Microsoft Defender und Microsoft Security-Lösungen
- Verwaltung von Intune und Mobile Device Management (MDM)
- Unterstützung bei Microsoft 365 Projekten und Weiterentwicklungen
- Automatisierung administrativer Prozesse mittels PowerShell

5. Backup-, Recovery- und Business Continuity Management

- Planung, Überwachung und Durchführung von Datensicherungen
- Regelmäßige Prüfung von Backup- und Wiederherstellungsprozessen
- Erstellung und Pflege von Notfall- und Wiederanlaufkonzepten
- Sicherstellung der Datenverfügbarkeit und Datenintegrität
- Durchführung von Restore-Tests und Dokumentation der Ergebnisse

Die Verantwortung für Datensicherung und Datensicherheit entspricht den Kernaufgaben der bisherigen Stellenbeschreibung.

6. System Monitoring und Betrieb

- Überwachung aller relevanten Server-, Netzwerk- und Cloud-Systeme

- Analyse von Fehlern und Störungen
- Durchführung von Wartungsarbeiten und Updates
- Sicherstellung der Verfügbarkeit geschäftskritischer Systeme
- Kapazitätsplanung und Performanceoptimierung
- Proaktive Erkennung und Vermeidung von Systemausfällen

7. IT-Service und Anwenderbetreuung

- Incident Annahme
- 2nd- und 3rd-Level-Support für Anwender
- Unterstützung bei Hard- und Softwareproblemen
- Installation und Konfiguration von Endgeräten
- Betreuung von mobilen Endgeräten
- Beratung der Fachabteilungen bei IT-relevanten Fragestellungen
- Unterstützung bei Einführungen neuer Systeme und Anwendungen

8. IT-Dokumentation und Compliance

- Kontinuierliche Pflege der IT-Dokumentation
- Dokumentation von Systemlandschaften, Netzwerken und Sicherheitskonzepten
- Dokumentation von Änderungs-, Incident- und Berechtigungsmanagement
- Pflege von Betriebs-, Notfall- und Sicherheitsdokumentationen
- Unterstützung bei internen und externen Audits
- Sicherstellung der Nachvollziehbarkeit aller wesentlichen IT-Prozesse

9. IT-Projekte und Weiterentwicklung

- Mitarbeit bei IT-Infrastrukturprojekten
- Bewertung neuer Technologien und Lösungen
- Unterstützung bei der IT-Budget- und Beschaffungsplanung
- Zusammenarbeit mit externen Dienstleistern
- Erstellung technischer Konzepte und Entscheidungsvorlagen
- Aktive Weiterentwicklung der IT-Landschaft und Sicherheitsarchitektur

10. Einzelaufträge

Der Stelleninhaber nimmt nehmen den o.g. Aufgaben nach Anweisung der vorgesetzten Stelle Einzelaufträge war, die dem Wesen nach zu dem Aufgabenbereich gehören, oder welche sich aus der betrieblichen Notwendigkeit ergeben. Er ist grundsätzlich verpflichtet nach entsprechender Information an Veranstaltungen und Arbeitskreisen auf Anweisung teilzunehmen.

V. Kompetenzen und Befugnisse

- Selbstständige Bearbeitung der übertragenen Aufgaben
- Technische Entscheidungsbefugnis innerhalb definierter IT-Standards
- Steuerung externer Dienstleister im Verantwortungsbereich
- Mitwirkung bei Beschaffungsentscheidungen und Technologieauswahl

- Eskalationsrecht bei Sicherheitsvorfällen und kritischen Systemstörungen

VI. Anforderungen an die Position

1. Fachliche Qualifikation

- Abgeschlossene Ausbildung als Fachinformatiker Systemintegration, IT-Systemelektroniker oder vergleichbare Qualifikation
- Alternativ abgeschlossenes Studium der Informatik oder Wirtschaftsinformatik
- Mehrjährige Berufserfahrung in der IT-Systemadministration

2. Fachkenntnisse

- Sehr gute Kenntnisse in Windows Server Administration
- Sehr gute Kenntnisse in Microsoft 365 und Entra ID
- Erfahrung mit Firewalls und Netzwerksicherheit
- Kenntnisse in Virtualisierungstechnologien (VMware, Hyper-V o. ä.)
- Erfahrung mit Backup- und Recovery-Lösungen
- Kenntnisse in IT-Security-Standards und Compliance-Anforderungen
- Gute PowerShell-Kenntnisse von Vorteil
- Erfahrung mit Endpoint-Management und Microsoft Intune
- Erfahrung mit XDR Systemen von Vorteil

3. Persönliche Kompetenzen

- Analytisches und strukturiertes Denken
- Hohes Sicherheits- und Qualitätsbewusstsein
- Eigenverantwortliche und lösungsorientierte Arbeitsweise
- Kommunikationsstärke und Serviceorientierung
- Teamfähigkeit und Zuverlässigkeit
- Bereitschaft zur kontinuierlichen Weiterbildung

VII. Erfolgskennzahlen (KPIs)

- Systemverfügbarkeit ≥ 99,5 %
- Erfolgreiche Backup- und Restore-Tests
- Einhaltung der Security- und Compliance-Anforderungen
- Dokumentationsgrad der IT-Systeme
- Reaktions- und Lösungszeiten bei Incidents
- Erfolgreiche Umsetzung von IT-Sicherheitsmaßnahmen
- Anwenderzufriedenheit im IT-Support