



KONTAKT

✉ christian.erben@degit.de
☎ +49 151 65172525
💻 christianerben.eu
🌐 [/christian-erben-828a08330/](https://www.linkedin.com/in/christian-erben-828a08330/)
🔗 [/Christian_Erben](https://github.com/Christian_Erben)
📅 06.07.1983
📍 Traminerweg 9
68309 Mannheim

SPRACHEN

🗣 Deutsch (Muttersprache)
🗣 Englisch (B2)

Christian Erben

Ich verfüge über langjährige Erfahrung in der System- und Netzwerkadministration, mit Schwerpunkt auf dem Design und der Absicherung komplexer, redundanter Infrastrukturen. Dazu zählen professionelles Firewall-Management, die Planung sicherer Netzwerkarchitekturen sowie fundierte Kenntnisse klassischer und anspruchsvoller Protokolle und Plattformen. Ergänzend bringe ich umfangreiche Praxis in der Linux-Administration, in sicherheitsorientierten Betriebsprozessen und im Aufbau strukturierter Security-Mechanismen wie IAM, ISMS sowie Incident- und Vulnerability-Management mit.

PROFIL

Als erfahrener IT-Engineer mit über 18 Jahren Praxis in Enterprise-Umgebungen verbinde ich tiefes technisches Know-how mit einem klaren Fokus auf Informationssicherheit und robuste Betriebsprozesse. Mein Schwerpunkt liegt auf der Gestaltung, dem Betrieb und der Absicherung komplexer Netzwerk- und Plattformarchitekturen. Dazu gehören insbesondere Firewall-Management, die Planung sicherer und segmentierter Netzwerke sowie umfangreiche Kenntnisse zu klassischen und auch exotischen Netzwerkprotokollen und verschiedensten Netzwerkprodukten.

Neben meiner Netzwerkerfahrung arbeite ich seit vielen Jahren intensiv mit Linux-Systemen und betreue sowohl klassische Serverumgebungen als auch containerisierte Plattformen. Diese technische Grundlage kombiniere ich mit strukturierten Ansätzen aus dem Informationssicherheitsmanagement, der Entwicklung von Security-Policies und dem Aufbau wirksamer Sicherheitsprozesse.

SECURITY & COMPLIANCE / GOVERNANCE

Informationssicherheitsmanagement (ISMS)

- Aufbau und Pflege von Sicherheitsrichtlinien (Policies, SOPs, Verfahrensanweisungen)
- Ableitung und Umsetzung organisatorischer und technischer Sicherheitsmaßnahmen
- Kontinuierliche Weiterentwicklung sicherer Betriebsprozesse

Security Governance

- Definition und Etablierung von Sicherheitsstandards für Infrastruktur- und Plattformbetrieb
- Dokumentation, Prozessgestaltung und Sicherstellung einer einheitlichen Policy-Anwendung
- Erstellung und Pflege sicherheitsrelevanter Betriebskonzepte

BSI IT-Grundschutz

- Nutzung der Grundschutz-Methodik zur Strukturierung und Bewertung von Sicherheitsmaßnahmen
- Unterstützung beim Aufbau sicherer Betriebsprozesse nach anerkannten Standards

Identity & Access Management (IAM)

- Rollen- und Berechtigungskonzepte (RBAC)
- Rechteprüfung, Rezertifizierung und Funktionstrennung
- Privileged Access Management (PAM)

Incident & Vulnerability Management

- Aufbau und Pflege strukturierter Prozesse für Incidents & Security Findings
- Priorisierung, Bearbeitung und Dokumentation sicherheitsrelevanter Vorfälle
- Operatives Schwachstellenmanagement (inkl. Patch-Planung und Follow-up)

BERUFSERFAHRUNG

Vorstandsmitglied

DEGIT AG

Apr 2020 - Heute

Hockenheim, Germany

- Vorstandsmitglied mit Fokus auf Datenschutz, Informationssicherheit und Netzwerkstrategie für mittelständische Kund:innen.
- Vernetzt Kund:innen mit Spezialist:innen aus dem DEGIT-Expertennetzwerk und koordiniert interdisziplinäre Beratungsteams.
- Überwacht die Konzeption sicherer, redundanter Infrastrukturen einschließlich Firewall-Konzepten, VPN-Lösungen (IPv6, Zero Trust, Zero-Config VPN, etc.) und Backup-Strategien.
- Einführung eines unternehmensweiten Security-Governance-Frameworks inkl. Policy-Design und Access Governance
- Durchführung strukturierter Risikoanalysen und Ableitung technischer Sicherheitsmaßnahmen
- Entwicklung sicherer Betriebsprozesse (Least Privilege, Logging, Monitoring, Rollenmodelle)
- **Erfolg: Aufbau eines Governance-Rahmens, der Netzwerksicherheit, Datenschutz und Compliance für neue Kundenprojekte bündelt.**

Compliance

Sicherheitsstrategie

Netzwerke

Beratung

Compliance

M365

Cloudflare

Supabase

Azure

IPv6

- Verwaltung und Prüfung von Netzwerkberechtigungen zur Gewährleistung korrekter und sicherer Zugriffskontrollen im Unternehmensnetz.
- Kontinuierliche Bereinigung veralteter Regeln zur Reduktion der Komplexität und zur Einhaltung interner Richtlinien.
- Unterstützung von IT-Projekten mit Netzwerkwissen, damit Architekturen zu aktuellen Topologien und Sicherheitsstandards passen.
- Pflege detaillierter Netzwerkdokumentationen zu Topologie, Richtlinien und Sicherheitsprotokollen.
- Koordination von Planung und Umsetzung von Changes mit Infrastruktur-, Sicherheits- und Applikationsteams.
- Betrieb von Proxy-Infrastrukturen und Monitoring von Netzwerkpfaden inklusive IPSec-Tunneln und SD-WAN-Verbindungen.
- Unterstützung bei der Einführung cloudbasierter Sicherheitsdienste wie Prisma SSE.
- Verantwortlich für Identity & Access Management (IAM) und Rechteprüfung im Enterprise-Umfeld
- Erstellung und Pflege sicherheitsrelevanter Prozesse und Dokumentationen
- Sicherstellung konsistenter Policy-Anwendung in komplexen Netzwerk- und Infrastrukturmgebungen
- **Erfolg: Reduktion der Firewall-Regelkomplexität von 5.000 auf unter 1.000 Einträge für mehr Transparenz und Performance.**
- **Erfolg: Migration von Palo Alto zu Fortinet und Übernahme komplexer Sicherheitsrichtlinien ohne Betriebsunterbrechung.**
- **Erfolg: Implementierung von IPv6 im gesamten Unternehmen, Zukunftssicherung des Netzwerks.**
- **Erfolg: Ausrollen sicherer SD-WAN-Anbindungen für Außenstandorte zur Verbesserung von Stabilität und Transparenz der Netzwerkkommunikation.**
- **Erfolg: Einführung von Microsoft-Azure-Diensten in die Infrastruktur bei gleichzeitiger Sicherstellung compliantem hybriden Betrieb.**

Firewall-Management

SD-WAN

IPSec

Proxy

Azure

IPv6

Change Management

Dokumentation

Cloud Security

KI-Trainingsplattform & Evaluierung von KI-Werkzeugen

DEGIT AG

Aug 2025 - Okt 2025

Hockenheim, Germany

- Konzeption und Aufbau einer internen KI-Trainingsplattform für den Unternehmensseinsatz mit Fokus auf EU-AI-Act-Compliance und praxisnahe Befähigung der Teams.
- Bewertung und Entscheidungsvorlage zum Vergleich führender KI- und Automatisierungsplattformen hinsichtlich Datenschutz, Zuverlässigkeit, API-Integration und Governance-Tauglichkeit.
- Evaluierung aufkommender agentischer KI-Workflows zur mehrstufigen Aufgabenorchestrierung und deren Integration in Unternehmensautomatisierungsumgebungen.
- **Erfolg: Analysiert und bewertet: OpenAI ChatGPT, OpenAI Open-Weight GPT-OSS, Microsoft Copilot, Perplexity, Anthropic Claude, Apple Foundation, z.AI GLM, n8n, make.com und Zapier.**
- **Erfolg: Entwicklung eines modularen Lernplattform-Prototyps mit Supabase- und Cloudflare-Integration, rollenbasierten Inhalten und Fortschrittsverfolgung.**
- **Erfolg: Erstellung eines vergleichenden Entscheidungsrahmens zur Unterstützung der KI-Einführungsstrategie des Unternehmens.**

KI-Evaluierung KI-Training EU AI Act Supabase Cloudflare Automatisierung
n8n make.com Zapier OpenAI Apple Foundation Anthropic Claude
Microsoft Copilot Perplexity z.AI GLM Agentische KI
Unternehmensautomatisierung Cursor Claude Code OpenAI Codex

Linux-Systemadministrator / Nagios-Administrator

Schwarz IT GmbH & Co. KG

Apr 2018 - Dez 2018

Weinsberg, Germany

- Betrieb großskaliger Umgebungen mit 15.000 physischen Servern und 50.000 virtuellen Maschinen.
- Automatisierte Bereitstellung von Servern, Applikationen und Konfigurationen über Puppet und Ansible.
- Sicherstellung der Hochverfügbarkeit durch strukturiertes Patchmanagement und Monitoring.
- Beratung von Projekten zur sicheren Infrastrukturkonzeption und Integration in bestehende Monitoring-Prozesse.
- **Erfolg: Beschleunigung der Server-Rollouts durch Automatisierung von Golden Images und Compliance-Checks.**

Linux Automatisierung Monitoring Hochverfügbarkeit Puppet Ansible
IPv6

Linux-Systemadministrator

Deutsche Vermögensberatung AG

Feb 2011 - Dez 2017

Frankfurt am Main, Germany

- Administration von 1.000 physischen Servern und 2.000 virtuellen Maschinen in einem stark regulierten Umfeld.
- Automatisierte Serverinstallationen und Konfigurationsworkflows mit Puppet und Ansible.
- Betrieb von Enterprise-E-Mail-Plattformen mit Dovecot und Postfix inklusive Archivierungslösungen.
- Implementierung von Storage-Lösungen wie Ceph und Cloud Storage für skalierbare Datendienste.
- **Erfolg: Aufbau einer Mail-Archivierungsplattform, die Langzeit-Compliance sicherstellte und eDiscovery vereinfachte.**
- **Erfolg: Konzeption und Implementierung von IPv6 im Netzwerk-Perimeter zur Sicherstellung der externen Erreichbarkeit.**

Linux E-Mail Automatisierung Storage Puppet Ceph IPv6

FÄHIGKEITEN & TECHNOLOGIEN

Sicherheit

Firewall Engineering (Fortinet, Palo Alto) Proxy-Management
Secure Web Gateways Access-Governance Change-Governance
Incident-Management Problem-Management

Infrastruktur

Linux-Administration Linux-Distributionen (Debian, Ubuntu, RHEL)
Hochverfügbarkeit Redundanz & Failover IPv6 & Routing
VPN & Sichere Konnektivität Monitoring Troubleshooting

Tools & DevOps

Bash / Shell Skripte paperless-ngx Git Cursor Postfix / Dovecot
Bind / Unbound Squid Proxy HAProxy Docker Caddy

Management

Change Management Teamübergreifende Koordination
Stakeholder-Kommunikation Technische Dokumentation

KI

KI-gestütztes Troubleshooting Agentische KI Multimodale KI Kausale KI
Lovable OpenAI / ChatGPT Anthropic / Claude Google / Gemini
KI-Ethik & Governance

Compliance

Regulatory Compliance (IT-Compliance) Audit-Readiness & Policy-Enforcement
Kontrollumgebungen im Finanzsektor

AUSGEWÄHLTE PROJEKTE

Optimierung der Firewall-Regelwerke

Verschlinkung der unternehmensweiten Firewall-Regelwerke durch Analyse von über 5.000 Objekten, Konsolidierung von Dubletten und Einführung eines Lebenszyklus für inaktive Regeln. Das Ergebnis: bessere Performance, Lesbarkeit und Auditfähigkeit.

Firewall Governance Automatisierung

Migration von Palo Alto zu Fortinet

Planung und Umsetzung einer Plattformmigration mit Überführung komplexer Objekte und Richtlinien nach Fortinet bei laufendem Betrieb. Einführung neuer Templates für nachhaltige Richtlinienhygiene.

Migration Fortinet Change Management

SD-WAN Rollout für Außenstandorte

Anbindung von Außenstandorten per SD-WAN, Definition von Redundanzkonzepten und Abstimmung des Monitorings für transparente Betriebsabläufe über alle Pfade.

SD-WAN Netzwerke Monitoring

Azure-Integration für hybride Infrastruktur

Einführung von Microsoft-Azure-Diensten in eine On-Prem-Umgebung inkl. Koordination von Netzwerkanbindung, Identity-Integration und Sicherheits-Baselines.

Azure Hybride Cloud Security