



## REACH ME AT

- [christian.erben@degit.de](mailto:christian.erben@degit.de)
- [+49 151 65172525](tel:+4915165172525)
- [christianerben.eu](http://christianerben.eu)
- [/christian-erben-828a08330/](https://www.linkedin.com/in/christian-erben-828a08330/)
- [@Christian\\_Erben](https://twitter.com/Christian_Erben)
- 06.07.1983
- Traminerweg 9  
68309 Mannheim

## LANGUAGES

- German (Native)
- English (B2)

# Christian Erben

I have many years of experience in system and network administration, with a focus on designing and securing complex, redundant infrastructures. This includes professional firewall management, planning secure network architectures, as well as solid knowledge of classic and advanced protocols and platforms. Additionally, I bring extensive practice in Linux administration, security-oriented operational processes, and the establishment of structured security mechanisms such as IAM, ISMS, as well as incident and vulnerability management.

## PROFILE

As an experienced IT engineer with over 18 years of practice in enterprise environments, I combine deep technical expertise with a clear focus on information security and robust operational processes. My focus lies on designing, operating, and securing complex network and platform architectures. This includes in particular firewall management, planning secure and segmented networks, as well as extensive knowledge of both classic and exotic network protocols and various network products.

In addition to my network experience, I have been working intensively with Linux systems for many years and manage both classic server environments and containerized platforms. I combine this technical foundation with structured approaches from information security management, the development of security policies, and the establishment of effective security processes.

## SECURITY & COMPLIANCE / GOVERNANCE

### Information Security Management (ISMS)

- Establishment and maintenance of security policies (Policies, SOPs, procedures)
- Derivation and implementation of organizational and technical security measures
- Continuous development of secure operational processes

### Security Governance

- Definition and establishment of security standards for infrastructure and platform operations
- Documentation, process design and ensuring uniform policy application
- Creation and maintenance of security-relevant operating concepts

### BSI IT-Grundsatz

- Use of Grundsatz methodology to structure and evaluate security measures
- Support in establishing secure operational processes according to recognized standards

### Identity & Access Management (IAM)

- Role and permission concepts (RBAC)
- Rights review, recertification and separation of functions
- Privileged Access Management (PAM)

### Incident & Vulnerability Management

- Establishment and maintenance of structured processes for incidents & security findings
- Prioritization, processing and documentation of security-relevant incidents
- Operational vulnerability management (including patch planning and follow-up)

## EXPERIENCE

### Member of the Board

**DEGIT AG**

Apr 2020 - Present

Hockenheim, Germany

- Board member focusing on data protection, information security, and network strategy for SME clients.
- Connects clients with specialists from DEGIT's expert network and coordinates interdisciplinary consulting teams.
- Oversees the design of secure, redundant infrastructures including firewall concepts, VPN solutions, and backup strategies.
- Introduction of a company-wide security governance framework including policy design and access governance
- Conducting structured risk analyses and deriving technical security measures
- Development of secure operational processes (Least Privilege, Logging, Monitoring, Role Models)
- **Achievement: Established a governance framework aligning network security, privacy, and compliance requirements for new customer projects.**

Compliance   Security Strategy   Networking   Consulting   Compliance   M365  
Cloudflare   Supabase   Azure

### Network Security / Management

**Deutsche Vermögensberatung AG**

Oct 2019 - Present

Frankfurt am Main, Germany

- Manage and review network permissions to maintain accurate, secure access controls across the enterprise.
- Continuously clean up legacy rules to reduce complexity and ensure compliance with internal policies.
- Support IT projects with network expertise, ensuring architectures align with current topologies and security standards.
- Maintain detailed network documentation covering topology, policies, and security protocols.
- Coordinate change planning and implementation with infrastructure, security, and application teams.
- Operate proxy infrastructures and monitor network paths including IPSec tunnels and SD-WAN links.
- Support the introduction of cloud-based security services such as Prisma SSE.
- Responsible for Identity & Access Management (IAM) and rights review in enterprise environments
- Creation and maintenance of security-relevant processes and documentation
- Ensuring consistent policy application in complex network and infrastructure environments
- **Achievement: Reduced firewall rule complexity from 5,000 to fewer than 1,000 entries for greater transparency and performance.**
- **Achievement: migration from Palo Alto to Fortinet, translating complex security policies without service interruption.**
- **Achievement: Rolled out secure SD-WAN connectivity for branch offices, improving stability and visibility of network communication.**
- **Achievement: Introduced Microsoft Azure services into the infrastructure while ensuring compliant hybrid connectivity.**

Firewall Management   SD-WAN   IPSec   Proxy   Azure   Change Management  
Documentation   Cloud Security

## AI Training Platform & AI Tools Evaluation

DEGIT AG

Aug 2025 - Oct 2025

Hockenheim, Germany

- Design and implementation of an internal AI training platform for corporate use, focusing on compliance with the EU AI Act and practical enablement of teams.
- Evaluation and decision paper comparing leading AI and automation platforms with regard to data protection, reliability, API integration, and governance readiness.
- Assessment of emerging agentic AI workflows for multi-step task orchestration and their integration into enterprise automation environments.
- Achievement: Analyzed and benchmarked: OpenAI ChatGPT, OpenAI Open-Weight GPT-OSS, Microsoft Copilot, Perplexity, Anthropic Claude, Apple Foundation, z.AI GLM, n8n, make.com, Zapier.
- Achievement: Developed a modular learning platform prototype with Supabase and Cloudflare integration, role-based content, and progress tracking.
- Achievement: Produced a comparative decision framework supporting the company's AI adoption strategy.

AI Evaluation    AI Training    EU AI Act    Supabase    Cloudflare    Automation    n8n  
make.com    Zapier    OpenAI    Apple Foundation    Anthropic Claude  
Microsoft Copilot    Perplexity    z.AI GLM    Agentic AI    Enterprise Automation  
Cursor    Claude Code    OpenAI Codex

## Linux Systems Administrator / Nagios Administrator

Schwarz IT GmbH & Co. KG

Apr 2018 - Dec 2018

Weinsberg, Germany

- Operated large-scale environments with 15,000 physical servers and 50,000 virtual machines.
- Automated provisioning of servers, applications, and configurations via Puppet and Ansible.
- Ensured high availability through structured patch management and monitoring.
- Advised projects on secure infrastructure design and integration into existing monitoring processes.
- Achievement: Accelerated server rollout cycles by automating golden-image provisioning and compliance checks.

Linux    Automation    Monitoring    High Availability    Puppet    Ansible

## Linux Systems Administrator

Deutsche Vermögensberatung AG

Feb 2011 - Dec 2017

Frankfurt am Main, Germany

- Administered 1,000 physical servers and 2,000 virtual machines in a highly regulated environment.
- Automated server installation and configuration workflows using Puppet and Ansible.
- Operated enterprise email platforms with Dovecot and Postfix including archiving solutions.
- Implemented storage solutions such as Ceph and cloud storage for scalable data services.
- Achievement: Delivered a mail archiving platform that ensured long-term compliance and simplified eDiscovery.

Linux    Email    Automation    Storage    Puppet    Ceph

## SKILLS & TECHNOLOGIES

### Security

Firewall Engineering (Fortinet, Palo Alto)   Proxy Management

Secure Web Gateways   Access Governance   Change Governance

Incident Management   Problem Management

### Infrastructure

Linux Administration   Linux Distributions (Debian, Ubuntu, RHEL)   High Availability

Redundancy & Failover   IPv6 & Routing   VPN & Secure Connectivity   Monitoring

Troubleshooting

### Tools & DevOps

Bash / Shell Scripting   paperless-ngx   Git   Cursor   Postfix / Dovecot

Bind / Unbound   Squid Proxy   HAProxy   Docker   Caddy

### Management

Change Management   Cross-team Coordination   Stakeholder Communication

Technical Documentation

### AI

AI-assisted Troubleshooting   Agentic AI   Multimodal AI   Causal AI   Lovable

OpenAI / ChatGPT   Anthropic / Claude   Google / Gemini   AI Ethics & Governance

### Compliance

Regulatory IT Compliance   Audit-Readiness & Policy Enforcement

Financial Sector Control Environments

## HIGHLIGHTED PROJECTS

### Firewall Rulebase Optimisation

Streamlined enterprise firewall rulebases by analysing 5,000+ objects, consolidating duplicates, and establishing a lifecycle for dormant rules. The result improved performance, readability, and audit readiness.

Firewall   Governance   Automation

### Palo Alto to Fortinet Migration

Planned and executed a platform migration, translating complex objects and policies into Fortinet while keeping services online. Introduced new templates for ongoing policy hygiene.

Migration   Fortinet   Change Management

### SD-WAN Branch Rollout

Connected branch offices via SD-WAN, defined redundancy concepts, and aligned monitoring to ensure transparent operations across all paths.

SD-WAN   Networking   Monitoring

### Azure Integration for Hybrid Infrastructure

Introduced Microsoft Azure services into an on-prem environment, coordinating network connectivity, identity integration, and security baselines.

Azure   Hybrid Cloud   Security