Christian
Enderle
Technischer IT-Manager

Kontakt & persönliches

go-digital@ds6.eu

Eckdaten:

Geburtsdatum: 08.09.1989
Staatsangehörigkeit: dt.
Standort: großteils Europa
Zahlungsziel: 14 Tage
Führerschein: Klasse B (PKW)

Sprachen:
Deutsch – Muttersprache
English – verhandlungssicher

Projekterfahrung:
Projektleitend und begleitend.
Kommunikation und Abstimmung.
Leitend und begleitend.
Intern ausführend, extern ausführend. Intern leitend, extern leitend, extern beratend.

KMU, branchenneutral.
Mitarbeiterumfang, direkt: 5-1.00, indirekt (Teilbereich) bis ca. 45.000

Art der Betriebe: Familienbetrieb, Konzern,
Start-Up.

Studienabschluss: Keiner
Studienfach: Wirtsch.-Inform.
Studienart: Bachelor of Science
Abbruchgrund: Leben als Studienfläche, Autodidakt

Schulabschluss: Allg. Abitur
Institut: Abendgymnasium
Jahr d. Abschlusses: 2013

Ausbildung: Fachinformatiker
Institut: IHK Ulm
Jahr des Abschlusses: 2010

Stand Lebenslauf: 2026/03/06.1

Schönen guten Tag!

Vorab möchte ich mich für Ihre Zeit bedanken, die Sie sich für meinen Lebenslauf nehmen werden.

Sie suchen nach einer Person:

- mit gut über fünfzehn Jahren praktischer Erfahrung in Tiefe und Breite der IT-Umsetzung und gleichzeitigem Unternehmertum? (- privat gut das doppelte)
- die das Prinzip CG-BOM (Consult-Design-Build-Operate-Manage) lebt?
- mit planerischer, beratender und umsetzender Erfahrung
- die branchenneutral arbeitet, branchenspezifische Elemente aber nicht unbeachtet lässt
- praktischem Wissen in Datenschutz- und Sicherheits-, Lizenzierungs & /-rechtlichen Fragen. Der dies zur Bewertung Ihrer Umgebungmiteinbringen kann und will? *(keine rechtl. Beratung!)*
- *Beratend, planend und Umsetzend mit Microsoft, SaaS, Closed Source, sowie Open Source Vertrautheit.*
- die praktisches Know-How im Umgang mit Mitarbeitern, Share und Stakeholdern der IT und Unternehmen einbringt?
- Mit eigenem Enthusiasmus, der die Projekte langfristig für alle Involvierten vorteilhaft umsetzen will?

Wenn das der Fall ist, müssen Sie nicht weitersuchen - Wie Sie meinem folgenden Lebenslauf entnehmen können, bringe ich diese Fähigkeiten in der Breite in kurz- oder, bevorzugt langfristigen Projekten gerne ein.

Ich freue mich auf unseren Austausch, wie ich meine Fähigkeiten auch zu Ihrem Vorteil in Ihr Unternehmen einbringen kann - Zur Vereinbarung eines Gesprächstermins erreichen Sie mich am besten per E-mail (enderle@ds6.eu).

Ich melde mich auf jeden Fall bei Ihnen und freue mich auf das aufkommende Projekt und die ergiebige Zusammenarbeit.

Mit besten Grüßen,
Christian Enderle

Anlagen

- ❖ Ausbildung und absolvierte Schulungen und Lehrgänge
- ❖ Projektübersicht

Ausbildung / Zertifikate (seit 2015)

10/2020 – heute	Studium des Wirtschaftsrechts Fokussierung auf IT-Recht und Datenschutzrecht, soweit möglich projektbegleitend
10/2012 – 07/2018	Studium der Wirtschaftsinformatik Kooperationsstudiengang Hochschule Ulm/Neu-Ulm, Abbruch durch Projektauslastung bedingt
03/2016	IT-Service Management ITIL3 Foundation Cert-No. 03971871-01-X4LD
06/2018	„Projekt- und Teammanagement Professional“ durch PMC-Sattler Projektmanagement-Professional / Guideline / Phasenmodell und Scrumvertiefung Teamentwicklung und -führung
	Sowie andere Zertifizierungen, bspw. für VMware (VCTP), Sophos (CE, CA), 3cx, Fortinet NSE (x)…
	Größtenteils autodidaktisch/Selbststudium, eigene Proof of Concepts

praktische berufliche Erfahrung (Ausschnitte seit 2010)

Vorweg möchte ich anmerken, dass diese Liste der Zusammenarbeit mit Geschäftspartnern nur ein **Ausschnitt** sein kann, um Ihnen einen **Abriss** zu geben. Jedes Projekt hat dabei seine ganz besonderen Herausforderungen, die sowohl planerischer als auch technischer Natur sein können. Ich freue mich über jede spannende Aufgabe, die in meinen Wirkkreis fällt. Noch mehr freue mich darüber, langfristig einen Beitrag zur Entwicklung des Projekts, der Unterstützung bei der IT-Strategie in Planung und Umsetzung eines jeden begleiteten Unternehmens beigetragen haben zu dürfen. Generell sind Projekte mit Kürzel versehen, um Ihnen die Rückfrage zu Inhalten und Hintergründe zu erlauben. Nur auf ausdrückliche Abstimmung mit dem betreffenden Kunden in Hinsicht auf den Kunden diesen als Referenz zu platzieren.

Sollten Sie spezifischere Fragen haben, kommen Sie gerne auf mich zu. Ich arbeite konstruktiver am „Objekt“. Sollten Sie Bedarf an englischsprachiger Unterstützung haben, so kann ich die relevanten Details auch hierfür ausarbeiten, sprechen Sie mich gerne hierauf an.

laufende Projekte/Tätigkeiten

Laufende Projekte sind derzeit abgeschlossene Teil-/Großprojekte, die allerdings regelmäßig für kleinere Rückfragen oder Standardmäßig für die IT-Entwicklung auf mich zurückgreifen. Der Aufwand hierfür hält sich – abgesehen von aufkommenden aktiven Projekten - im Rahmen von wenigen Stunden im Monat.

Die Sortierung erfolgt absteigend, aktuelle oder anhaltende Projekte sind oben sortiert.

08/2010 – heute Externe IT-Leitung / IT-Architekt; Mittelstand (MN)

- Komplettübernahme des internen IT-Managements mit Schnittstellenfunktionalität, Beratung und Support
- Aufnahme IST-Situation/Erarbeitung Soll-Definition
- Analyse, Erstellung und Umsetzung IT-Sicherheitsrichtlinie
- Systemhardening, Umsetzung neuer IT-Struktur mit getrennten Netzwerkabschnitten und VLANs
- Trennung Maschinenpark vom GF und Mitarbeiternetz
- Einsatz jew. aktueller, mehrstufiger Methoden zur Einbruchsprävention
- Live-Case: 1. GF erhält Schadsoftware per USB-Stick, der Zugriff auf Datei erfolgte, 2.ter GF öffnet USB-Stick ebenfalls, weder im Geschäftsführungsnetz, noch im sonstigen Firmenumfeld gab es einen Einbruch, noch negative Implikationen.
- Projektmanagement/Rettung bei im Scheitern befindl. Programmierprojekt Technikeinsatz:

HPE / Dell Server, HPE / Dell Clients
Sophos SG, HPE, Cisco Firewall und Switches
Microsoft AD 2003/2008R2/2019/2025
Microsoft Exchange 2010/2019 / SE
Mailarchivierung
Microsoft IIS (Internet Information Services) 2010-2019
Microsoft SQL Server, DBA, Datenbankverwaltung
Microsoft Hyper-V 2008-2025
Debian Linux (V6. bis aktuell)
Bash und Powershell Scripting
div. Closed und Open-Source, sowie Freeware (FOSS)
Backup: urbackup, Veeam, Selbstgescripted
Rollout Kaspersky und Ersatz Eset AV (Client/Server)
VoIP-TK, bitFarm DMS
Dienste: DNS, DHCP, TCP/IP, Subnetting, Firewalling, Routing, NextCloud
IT-Beratung, IT-Sicherheitsanalyse, IT-Architektur, SIEM, VLAN, WLAN,
Netzsegmentierung Remoteeinsatz: 95%

10/2012 – heute Externe IT-Leitung / IT-Architekt; Hotellerie (KS)

- Komplettübernahme der internen IT-Managements, „CIO“, „CISO“, System Engineer (2nd / 3rd Level zur Internen IT), Beratung und Support u.a per Ticketsystem
- Aufnahme IST-Situation/Erarbeitung Soll-Definition
- Umsetzung der zentralen Serverinfrastruktur inkl. Beschaffung
- Umsetzung Remotemöglichkeit
- Umsetzung IT-Sicherheitsrichtlinie, Systemhärtung
- Umsetzung neuer IT-Struktur mit getrennten Netzwerkabschnitten/VLANs
- Trennung Gästenetzwerk von Internen Netzwerken
- Ersatz bisheriger Klingeldraht-Kommunikation zwischen den Häusern auf wesentlich leistungsfähigere WLAN-Richtfunktechnologie.
- Einsatz neuer, mehrstufiger Methoden zur Einbruchsprävention
- Schnittstellenfunktionalität/Sourcing
- Unterrichtung und Planung auf Basis BDSG, DSGVO, BSI-Grundschutz
- Technikeinsatz:
  Dell Server, Dell Clients, Ruckus APs
  Sophos SG, HPE, Cisco Firewall und Switches
  Microsoft AD 2008R2/2019/2025
  Microsoft Exchange 2010/2019/ SE
  Microsoft Hyper-V 2008-2025
  Microsoft IIS (Internet Information Services) 2010 - 2025
  Debian Linux, FOSS (V6. Bis aktuell)
  FOSS-Evaluation
  Lizenzierung und Governance
  Systemmonitoring (Stack auf Basis check mk)
  Backup: urbackup, Veeam, Selbstgescripted
  Dienste: DNS, DHCP, TCP/IP, Subnetting, Firewalling, Routing, VoIP
  IT-Beratung, IT-Sicherheitsanalyse, IT-Architektur, SIEM, VLAN, WLAN,
  Netzsegmentierung und IT-Sicherheitsawareness schaffen, MariaDB, MySQL, InfluxDB, php, jquery
  Bash, PHP, SQL und Powershell Scripting
- Remoteeinsatz: 90%

05/2015 - heute Webhosting / Application Service Provider / Managed Services

- Komplettübernahme der internen IT-Verwaltung CEO, CIO, CISO
- Aufnahme IST-Situation/Erarbeitung Soll-Definition
- Umsetzung der zentralen Serverinfrastruktur inkl. Beschaffung
- Einsatz neuer, mehrstufiger Methoden zur Einbruchsprävention
- Schnittstellenfunktionalität/Sourcing
- erreichtes Umsetzungsziel jeweils A/A++ Ratings
- Zielsetzung und Planung auf Basis BDSG, DSGVO, BSI-Grundschutz
- Technikeinsatz:
  Dell Server, Dell Clients
  Sophos SG, HPE, Cisco Firewall und Switches
  Microsoft AD 2016-2022
  Microsoft Hyper-V 2012R2-2025
  Exchange Server 2013-2019
  Office 365, Microsoft 365, Teams, ToDo, Lists, Sharepoint
  Mailarchivierung
  Debian Linux (V6. Bis aktuell)
  Evaluation und Einsatz von Software (closed und Open), FOSS
  Zammad, elasticsearch,...
  Ubuntu Linux

FreeNas
Azure/AWS
Veeam
Lizenzierung und Governance
urBackup
NextCloud, SeaFile
eigenentwickeltes Backupsystem zum Remotebackup (abandoned seit 2018)
Microsoft Terminal-Services
Bash, PHP, SQL und Powershell Scripting
Systemmonitoring auf Basis des check_mk Stacks
Dienste: DNS, DHCP, TCP/IP, Subnetting, Firewalling, Routing, VoIP
IT-Beratung, IT-Sicherheitsanalyse, IT-Architektur, SIEM, VLAN, WLAN, Netzsegmentierung, Postfix, Apache2, nginx, PHP
KI-Integration, Ollama, div. Huggingface und Openrouter als Schnittstelle und MCP, Chatbot(s), Customer Onboarding Anbindung an OpenAI, Gemini, Anthroponic, ComfyUI, Web, Systemoptimierung und Selbstbetrieb.

- Remoteeinsatz: 95%

06/2018 - heute Ergänzung interne IT / IT-Beratung, Spezialmaschinenbau (RM)

- Hinzugezogen aufgrund von Netzsicherheitsproblemen
- Allgemein Managing System Engineer, Beratung und Support u.a per Ticketsystem
- Planung und Umsetzung VLAN-Struktur/Routing
- Beratung und Implementierung Firewalllösung, Systemhärtung
- Aufgrund positiven Projektverlaufs zügig als alleiniger Externer IT-Betreuer bestellt
- IT- und IT-Sicherheitstechnische Leitungs /Steuerungsfunktion („Stabsstelle“)
- Aufbau neue Serverinfrastruktur auf Basis Server 2016 (Da Release Server 2019 verspätet)
- Einrichtung Sicherheitsregelung, BSI-Grundschutz, DSGVO-Beratung
- Cloud-Remigration div. Dienste u.a Mailing von O365/Azure auf Exchange 2019
- Unterstützung bei der Absicherung der Spezialmaschinen
- Projektmanagement techn. Natur
- Projektsteuerung externer Dienstleister (Programmierung, Technik)
- Verhandlungsführer/Sourcing
- Technikeinsatz:
  Dell Server, Dell Clients
  Sophos SG, HPE, Ruckus Networking, Cisco Firewall und Switches
  Microsoft AD 2008R2-2025
  Microsoft Exchange 2010/2019, Migration von Office 365/Azure
  Mailarchivierung, Mailverschlüsselung
  NextCloud
  Einsatz von FOSS Software, sowie Lizenzierung und Governance
  Einrichtung, Troubleshooting, Wartung Datev
  Microsoft IIS (Internet Information Services) 2019
  Microsoft Terminal-Services Cluster unter 2019
  VMware Hyper-Visor 6.x, 7.x
  Backup: Veeam
  Microsoft SQL Server, DBA, Datenbankverwaltung, Debian, Ubuntu
  Dienste: DNS, DHCP, TCP/IP, Subnetting, Firewalling, Routing, VoIP, Linux, Php, MariaDB, MySQL, jquery
  Bash, PHP, SQL und Powershell Scripting
  IT-Beratung, IT-Sicherheitsanalyse, IT-Architektur, SIEM, VLAN, WLANNetzsegmentierung, SDSL, Glasfaser, 2nd und 3rd Level
- Remoteeinsatz: 100%

01/2020 – heute Netz-Neuaufbau mit erg. TK-Projekt, medizinischer Verbund (MLOS)

- Analyse Anforderungen und IST-Situation
- Prüfung der möglichen Realisierungswege, Beratung des IT-Leiters, Support
- Aufbau eines Grobkonzepts zum Netzrouting und Segmentierung
- Gegenprüfung und Diskussion auf Roll-Outfähigkeit über alle Standorte
- Ausrollen auf Standort „Alpha“ gemäß Soll-Definition.
- Abschluss, Tests.
- Beginn darauf aufbauendem TK-Projekt, Entstörung von 1,5 Jahre dauerndem Roll-Out-Projekt anhand von techn. Mängeln in Planung und Umsetzung in ca 1,5 Monaten gelöst. Kundenzufriedenheit erreicht
- Unterstützung bei der Absicherung der sensiblen Daten
- Beratung in Hinsicht auf BSI-Grundschutz, BDSG, DSGVO, medizin. Sonderanforderungen
- Projektmanagement techn. Natur
- LoadBalancing
- Technikeinsatz:
  Network-Troubleshooting

VLAN
Netzwerkschemaberatung und Umsetzung
priorisiert Open-Source Einsatz:
- pfSense
- FreeNas
- FOSS, Lizenzierung und Governance
- Planung High-Availability Network Infrastructure Datacenter
- ProxMox Virtualisierung
- Debian, Ubuntu Linux, SIEM, Netzwerk-Troubleshooting
- Cisco, Ruckus Switches
- 3cx Telefonanlage
- alt: bintec elmeg TK
- VMware vSphere 6 + 7, 8
- Veeam
- ProxMox V8 und V9
- OpenSense und pfSense

Remoteeinsatz: 100%

12 / 2020 – heute Projekt: Aufbau ASP-Struktur

- Analyse Anforderungen und IST-Situation
- Prüfung der möglichen Realisierungswege, Planung des Vorgehens
- Planung und Vorbereitung der Absicherung der sensiblen Daten
- Planung in Bezug auf BSI-Grundschutz, BDSG, DSGVO
- Projektmanagement techn. Natur
- Systemüberwachungsinfrastruktur (Monitoring) Intern/Extern
- IT-Governance, Planung und IT-Sicherheitsbacktests
- LoadBalancing
- Technikeinsatz:
  - Hyper-V 2016, 2022
  - Microsoft Terminal-Services Cluster unter 2019/2022
  - VMware
  - ProxMox PVE, Proxmox Backup Server
  - VMware vCenter
  - Citrix
  - Microsoft Exchange 2019
  - Windows, Office365 / Microsoft 365 / Azure AD
  - Cisco, Zyxel und HP Switches
  - Kubernetes
  - Sophos, Fortinet Firewalls/UTMs
  - Debian Linux, Nextcloud, SeaFile
  - NextCloud, div. FOSS und CSS, Lizenzierung und Governance
  - Microsoft IIS (Internet Information Services) 2022
  - nGinx, MariaDB, MySQL, varnish
  - IPv4 / IPv6 Networking
  - Zammad, elasticsearch,...

  Bash, PHP, SQL und Powershell Scripting
  Backup: Veeam
  Dienste: DNS, DHCP, TCP/IP, Subnetting, Firewalling, Routing, VoIP, check_mk, PHP, MySQL, MariaDB
  IT-Beratung, IT-Sicherheitsanalyse, VoIP, IT-Architektur, SIEM, Remote Work, Home Office, Hochverfügbarkeit, Failover, VLAN

10/2024 – heute Externe 3rd Level Unterstützung (CD-BOM)

- Analyse Anforderungen und IST-Situation
- Ziel Unterstützung im täglichen Support auf 2nd/3rd Level
- IT-Abteilung
- Planung und Vorbereitung der Absicherung der sensiblen Daten
- Planung in Bezug auf BSI-Grundschutz, BDSG, DSGVO
- Projektmanagement techn. Natur
- Systemüberwachungsinfrastruktur (Monitoring) Intern/Extern
- IT-Governance, Planung und IT-Sicherheitsbacktests
- LoadBalancing
- Technikeinsatz:
  - Hyper-V 2016, 2022
  - Microsoft Terminal-Services Cluster unter 2019/2022
  - VMware
  - ProxMox PVE, Proxmox Backup Server
  - VMware vCenter
  - Citrix

- Microsoft Exchange 2019
- Windows, Office365 / Microsoft 365 / Azure AD
- Cisco, Zyxel und HP Switches
- Kubernetes
- Sophos, Fortinet Firewalls/UTMs
- Debian Linux, Nextcloud, SeaFile
- NextCloud, div. FOSS und CSS, Lizenzierung und Governance
- Microsoft IIS (Internet Information Services) 2022
- nGinx, MariaDB, MySQL, varnish
- IPv4 / IPv6 Networking
- Zammad, elasticsearch,…

Bash, PHP, SQL und Powershell Scripting
Backup: Veeam
Dienste: DNS, DHCP, TCP/IP, Subnetting, Firewalling, Routing, VoIP, check_mk, Zabbix, PHP, MySQL, MariaDB
IT-Beratung, IT-Sicherheitsanalyse, VoIP, IT-Architektur, SIEM, Remote Work, Home Office, Hochverfügbarkeit, Failover, VLAN

Zeitlich abgegrenzte Projekte:

11 / 2024 – 07 / 2025 Externe beratende und Unterstützende Ergänzung der IT-Abteilung (ST)

- ❖ Generell Generalistisch und interdisziplinär, sowie eingebettet in das Kernteam „Infrastruktur“ mit Schnittstellen zum Helpdesk und ERP/SAP-Team
- ❖ Analyse der Umgebung auf Sicherheits- und konzeptioneller Schwachstellen
- ❖ Planung, Wartung und Optimierung der bestehenden VLAN-Infrastruktur
- ❖ Prüfung der Patchstände und dahingehende Optimierung und Aktualisierung mit gleichzeitiger Konfigurationsoptimierung
- ❖ Prüfung Windows-AD und Redesign der Gruppen- und Rechtestruktur
- ❖ Neuinstallation div. Systeme ausgehende von pre 2010 Systemen im Live-Betrieb unter Windows und Linux. Übertrag der Systemumgebungen auf aktuelle Laufzeiten.
- ❖ Troubleshooting, 2nd / 3rd Level
- ❖ Behebung von Leistungsengpässen
- ❖ Planung und Umsetzung eines neuen Backupbackends
- ❖ Vorantrieb der Cloud to On-Premise Migration um im wesentlichen unnötige Cloudkosten zu reduzieren.
- ❖ Aufbau eines PoC für Remotearbeit in der Fertigung, autark und mit absoluter Minimierung von Fehlern am Point-of-Work.
- ❖ Optimierung der globalen VPN-Struktur mit Fokus auf Absicherung und gleichzeitiger Integration (NAC) ins Kernsystem. (Backdoorschließung). Somit auch Homogenisierung der Netze. Begleitung des Roll-Outs.
- ❖ Steuerung und Begleitung von Lieferanten- und Eskalationsmeetings um div. Weak-Spots der bisherigen Struktur aus finanzieller und technischer Hinsicht aus der Welt zu schaffen, bzw zu straffen.
- ❖ Loginmechanismen, SSO, SAP, SSO, LDAPs
- ❖ Vorbereitung eines Patchkonzepts, um die Serversysteme kontinuierlich und durchgesetzt auf aktuellem Sicherheitsniveau halten zu können.
- ❖ Implementierung von PoCs für Alternativen zum bestehenden Monitoringtool PRTG: check_mk und zabbix.
- ❖ Begleitung und Initiierung von Daily, Strategie- und Krisenmeetings
- ❖ Technikeinsatz:
  - Microsoft Windows Server 2003 bis Server 2025
  - Microsoft SQL Server 201x, MySQL, postgresql, git
  - Microsoft Exchange 2019
  - Microsoft Terminal Services / Remote Desktop Services
  - PRTG Monitoring, check_mk, Zabbix Monitoringsysteme
  - Grafana Dashboard
  - VMware ESXI und vCenter inkl. Upgrade
  - Ubuntu Linux / Debian Linux
  - HPE Aruba Switches und Access-Points, sowie Management Controller
  - HPE 3par und Alletra Storagesysteme, sowie QNAP
  - HPE Server
  - Azure und Wazuh SIEM
  - Baramundi Management Software, Konfiguration, Wartung, Erweiterung
  - AutoCAD, Autodeployment
  - MacMon NAC, Konfiguration, Wartung, Optimierung, Routing
    Projektabriss macMon

    Implementierung und Ausrollen von MacMon am Hauptstandort, sowie Aufbau, Rückprüfung und Ergänzung der VLAN Struktur. Troubleshooting bestehender MacMon Instanzen und Optimierung der Struktur. Ergänzung der

Schnittstellen, sowie Neudefinition.

Ergänzend Ausrollen der MacMon Instanz im Blueprint und danach Live auf div. globale Aussenstellen, womit das dortige Security Level auf den Hauptstandort, inkl. interorganisatorischer Definition der Zuweisungen gehoben wurde.

- Zertifikatsausbringung optimiert und voran getrieben.
- CheckPoint, Stormshield und OPNsense Firewalls
- Veeam Backup und Backup für O365, Backupproxy, Immutable Backup
- Office 365, Azure AD und Azure Cloud
- MS Gruppenrichtlinien, Design, Harmonisierung, Entschlackung
- VPN, VLAN, Routing, Firewalling, Zoning (Design und Umsetzung)
- Lizenzierung und Governance, Hinweise auf IT-Sicherheitslücken
- WTware als Basis für die PXE Ausbringung von ThinClients nach minimal Effort am Produktionsarbeitsplatz
- Terminalserver Implementierung
- UDS Enterprise Deployment
- Powershell Scripting

06 / 2022 – 09 / 2024 IT-Beratung / IT-Neuaufbau (PF)

- Analyse Anforderungen und IST-Situation
- Migration von alter Domänenstruktur (200x) und Tobit auf Exchange 2019 und funktionaler Anbindung/Integration an MS365.
- Prüfung der möglichen Realisierungswege, Planung des Vorgehens
- Planung und Vorbereitung der Absicherung der sensiblen Daten
- Planung in Bezug auf BSI-Grundschutz, BDSG, DSGVO
- Projektmanagement techn. Natur
- IT-Governance, Planung und IT-Sicherheitsbacktests
- Technikeinsatz:
  - Hyper-V 2016, 2022
  - Microsoft Terminal-Services Cluster unter 2022
  - Microsoft Exchange 2019
  - Office365 / Microsoft 365 / Azure AD / Teams / SalesForce
  - Cisco, Zyxel und HP Switches
  - Sophos Firewalls/UTMs, sowie SecurePoint
  - Microsoft IIS (Internet Information Services) 2022
  - IPv4/IPv6
  - Backup Veeam und Wortmann Online Backup
  - NextCloud (FOSS)
  - Lizenzierung und Governance
  - ERP (Salesforce) Einrichtungsunterstützung
  - Absicherung Mailtransfer

  Dienste: DNS, DHCP, TCP/IP, Subnetting, Firewalling, Routing, VoIP, Gruppenrichtlinie, GPO, Powershell
  IT-Beratung, IT-Sicherheitsanalyse, VoIP, IT-Architektur, SIEM, Remote Work, Home Office, Hochverfügbarkeit, Failover, VLAN, PRTG

09 / 2018 – 10 / 2023 IT-Beratung / IT-Entwicklung, Managemententwickler (RY)

- Aufgrund von DSGVO-Anforderungen hinzugezogen
- IT- und IT-Sicherheitstechnische Leitungs- /Steuerungsfunktion („Stabsstelle“), System Engineer, Beratung und Support u.a per Ticketsystem
- Behebung von Mängeln in bisherigen Abläufen
- Behebung von potenziell kritischen DSGVO-Angriffsflächen
- Entwicklung interner IT, Kombination von on-Premise und Cloud-Lösungen
- Einbindung von Brachliegenden Ressourcen (CRM)
- Entwicklung von Work-Everywhere Konzepten (preCovid19)
- Einrichtung von zentralem Datenbestand
- Absicherung des Unternehmensnetzes
- Projektmanagement techn. Natur
- Schulung und Beratung in IT-Fragen
- Technikeinsatz:
  Dell Server, Dell Clients
  Sophos SG, Fortinet, Cisco Firewall und Switches
  Windows, Microsoft AD 2019
  Eset Antivirus (Client/Server)
  Microsoft Exchange 2019, O365 (Remigration), Microsoft 365, Lync, Skype. Teams
  Microsoft IIS (Internet Information Services) 2019

Microsoft Hyper-V 2019, VMware
Backup: Veeam
Lizenzierung und Governance
FOSS
LoadBalancing
Dienste: DNS, DHCP, TCP/IP, Subnetting, Firewalling, Routing, VoIP
IT-Beratung, IT-Sicherheitsanalyse, VoIP, IT-Architektur, SIEM, Remote Work, Home Office, Linux, Debian, Ubuntu, Php, MySQL, MariaDB, NextCloud, PowerShell

- Remoteeinsatz: 98%

KW 20 /2022 – KW 13 /2023

Projekt: Unterstützung IT/Linux Landschaft (SIE)

- Einsatz als 2nd / 3rd Level (Linux) System Engineer/Berater
- Überführung von nativen Installationen in virtuelle Umgebungen
- Beratung und Unterstützung in Hinsicht auf HA-Implementierung
- Testverfahren zur Evaluierung
- Beratung im IT-Sicherheitsumfeld / Protokollen / Absicherungen (u.a VPN/WLAN)
- Authentifizierungsberatung
- Begleitung der involvierten Teams, kritische Prüfung der Möglichkeiten und sich daraus ergebenden zukünftigen Fragestellungen („Prüfung auf Zukunftsfähigkeit“).
- Analytische Erfassung der Problemursachen mit Gegenüberstellung „Repair“ vs. „Rebuild“
- Technikeinsatz:
  - Windows VDI
  - proxMox Virtual Environment 7.x
  - pfSense Firewall anstatt ipTables
  - VPN: ipSec mit SmartCard Auth, WireGuard
  - LoadBalancing
  - Office 365, Teams Analyse im Einsatz unter Linux
  - Lizenzierung und Governance
  - FOSS Software
  - Citrix VDI // NetScaler
  - Azure/MS365 Anbindung an Linux Evaluiert
  - Bash, PHP, SQL und Powershell Scripting
  - Debian OS, Ubuntu, VMware, SIEM, 2FA, Gitlab, Ansible, Kubernetes

KW 16 / 2021 – KW 22 / 2022

Projekt: Analyse und Neuaufbau Terminalserver im multinationalen Umfeld (ZE)

- Einsatz als 2nd / 3rd Level (Microsoft) System Engineer/Berater + Support u.a per Ticketsystem
- Implizit IT-Stabsstelle mit extern stehender Steuerungs- und Beratungsfunktion
- Analyse des Umfelds im multihierarchischen und -nationalen Umfeld
- Troubleshooting lokaler und globaler Incidents, z.T FT/WE, Eskalation mit Problem-Identifikation an zuständige Teams
- Benutzerschulung im responsiven Umgang mit Systemen und Fehlern
- Begleitung der involvierten Teams, kritische Prüfung der Möglichkeiten und sich daraus ergebenden zukünftigen Fragestellungen („Prüfung auf Zukunftsfähigkeit“).
- Analytische Erfassung der Problemursachen mit Gegenüberstellung „Repair“ vs. „Rebuild“
- Hinwirkung auf Neuaufstellung, da zukunftsfähiger (Analyse ergebend)
- Hinwirkung zum Aufbau eines Proof of Concepts zur internen Evaluation der neuen Umgebung als Technikbenchmark
- Technikeinsatz:
  - Windows Terminal Services // Remote Desktop Services ab 2008 bis 2022
  - VMware ESXI
  - netApp Storage
  - TrueNAS/FreeNas
  - VMware vCenter
  - Microsoft Clusterfunktionen
  - SQL Server, Datenbankverwaltung
  - LoadBalancing
  - Office 365, Teams, Hybrid-Setup, Mailverschlüsselung
  - Citrix VDI, NetScaler, Apps, Gegenanalyse zu TS-Einsatz, u.a
  - Symantec AV, Fortinet, u.a
  - Lizenzierung und Governance
  - Azure/AWS
  - Integrity
  - PowerShell Scripting
  - Systemmonitoring mit Prometheus/Graphana, Zabbix abgelöst
  - Microsoft Server 2008 – 2016 (Analyse 2019, 2022)
  - Microsoft IIS (Internet Information Services) 2008 - 2016
  - Microsoft Terminal Services 2008, 2012R2, 2016

- fsLogix, 2FA, SIEM
-

Dienste: VDI, Terminal Server, Azure, Active-Directory, LDAP(s), Doors, Integrity, BCM, Gruppenrichtlinien, Rechteverwaltung, Remedy
Umfang: 45.000 Mitarbeiter, global
Remote, hauptsächlich English

KW 08-09 / 2021 Incidenthandling „Hafnium Hack“

betraf: insb. Neukunden aus Mittelstand: Maschinenbau, Medizin, Beratung, Kommunen u.a

- ungeplanter „Feuerwehreinsatz“ aufgrund globaler Attacken auf Exchange Server
- Prüfung des Hacks, Analyse der Vorgehensweise
- Analysierung von Exchange Installationen bei direkten und mittelbaren Kunden
- Isolierung von potentiell oder tatsächlich infizierten Systeme
- Bewertung von Angriffsvektoren und Zustandsanomalien, Prüfung der Systeme auf Webshells
- Korrespondenz mit Geschäftsleitung zur Risikobewertung aus allg. Systemsicherheits- und Datenabfluss, sowie DSGVO Sicht
- Systemhärtung im Nachgang
- Prüfung und Umsetzung des raschen Ersatzes
- Umsetzung von Sicherheitsmaßnahmen in jedem Fall, Härtung der Systeme, Bewertung von kritischen Einfalltoren
- Powershell Analysen
- Austausch mit Security-Abteilungen u.a Head of Security for Operations der Arvato Systems, Siemens,…
- Allgemeine Sicherheitstechnische Beratung über den Hack hinaus

  Dahinterliegender Gedanke: Ggf. Einsatz der durch NSA-Hack erfolgten Zero-Day-Lücken, unter Umständen nur „erste Attacke“.

  Dienste: Exchange 2013 – 2019, Office 365 Gegenschuss, Active-Directory, LDAP, u.a Sophos UTM, Fortigate LanCom, SecurePoint,… Virtualisierung, Server 2012R2 – 2019, div Firewalls, Proxy-Server, Web Application Firewall, Mailverschlüsselung, Awareness-Schulung

11 / 2020 - 04 / 2021 Exchange-Migration und Upgrade einer Kommune (GS)

- Analyse Anforderungen und IST-Situation als managing System Engineer
- Prüfung der möglichen Realisierungswege, Beratung des IT-Leiters
- Planung eines für die Benutzer störungsfreien Upgradepfads von Exchange 2010 auf Exchange 2019
- Unterstützung bei der Absicherung der sensiblen Daten
- Troubleshooting früherer Konfigurationen
- Beratung in Hinsicht auf BSI-Grundschutz, BDSG, DSGVO
- Projektmanagement techn. Natur
- Bereinigung von Altlasten
- Technikeinsatz:
  - Hyper-V 2016, 2019, VMware
  - Windows, Exchange 2010, 2013, 2019
  - Cisco Switches, Fortigate Firewalls, Mailarchivierung, Proxy, Mailverschlüsselung, Veeam-Backup
- Remoteeinsatz: 100% Hinweis: Verzögerung durch Komm. RZ, Corona und Wahlen
- Folgend 2nd /3rd Level Einsatz für interne IT bzw sekundären Dienstleister Umfang: 150 Mitarbeiter

10/2019 – 07/2020 IT-Restrukteur nach Ransomware-Angriff, Sicherheitsdienst (WS)

- Meldung um Jahreswende 2019/2020 in der Vorbereitungsphase für ein neues Projekt, Urlaubsabbruch, Rückreise zur Analyse
- Abriegelung des IT-Verkehrs zur Unterbindung weiter Ausbreitung
- Neuaufstellung der IT-Struktur, Beratung Unternehmensleitung
- Einbindung einer starken Firewall mit IDS/IPS und Mail-Scanfunktionalität
- Neuinstallation der Serverinfrastruktur mit aktueller Systemsoftware
- Implementierung getrennter Netze für ein mehrstufiges Sicherheitssystem, Hardening
- Beratung in Hinsicht auf DSGVO, BSI-Grundschutz und IT-Sicherheitsanforderungen an die Mitarbeiter
- Erarbeitung Rechtekonzept

- Einrichtung Sage, Datev, div. Branchensoftware
- Technikeinsatz:
  Dell / IBM Server
  Sophos SG Firewall
  Server 2008 / 2019
  Microsoft AD 2019
  Microsoft Exchange 2019, Migration von Microsoft O365, Hybrid
  Microsoft Azure / Amazon AWS
  Microsoft Hyper-V 2019
  Microsoft Terminal-Services unter 2019
  VMware HyperVisor 6.x, 7.x
- Dienste: DNS, DHCP, TCP/IP, Subnetting, Firewalling, Routing
  IT-Beratung, IT-Sicherheitsanalyse, IT-Architektur, White-Hat Hacking zur Quellenanalyse/Schadensbewertung
- Lizenzierung und Governance
- Remoteeinsatz: 100%
- Steuerung externer Dienstleister
  Umfang: 1.250 Mitarbeiter

11/2019 – 12/2020
04/2020; 07/2020

IT-Restrukteur / Renovator, Spezialelektronik (HS)

- Aufnahme IST-Situation/Erarbeitung Soll-Definition
- Troubleshooting Instabile und Ineffiziente IT-Struktur auf Basis 2012R2 und 2019, sowie Exchange 2016 und 2019
- Entwicklung der neuen IT-Struktur
- Umsetzung IT-Struktur unter AD2019 und Exchange 2019
- Gruppen und IT-Sicherheitsdefinition, Netzwerktrennung, Einführung Patchmanagement und VLANs
- Einrichtung Sage, Datev, div. Branchensoftware
- Technikeinsatz:
  HPE / IBM Server
  Sophos SG Firewall
  Microsoft AD 2016 / 2019
  Microsoft Exchange 2016 / 2019
  VMware Hypervisor ESXi 5.5, 6.x, 7.x
- Dienste: DNS, DHCP, TCP/IP, Subnetting, Firewalling, Routing
  IT-Beratung, IT-Sicherheitsanalyse, IT-Architektur
- Remoteeinsatz: 100%
  Umfang: 150 Mitarbeiter

07/2018 – 05/2020

Systemrettung und Restauration im Einzelhandel (SD)

- Kunde wünschte die Übernahme der Betreuung einer fremdprogrammierten Website und Webshopkonstrukts unter Docker
- Übernahme zeigte, dass das System seit geraumer Zeit nicht gewartet, geschweige geupdatet und massiv unsicher war. Ferner war der Host zu schwach.
- Erarbeitung der Umgebung, Analyse der Zusammenhänge/Erarbeitung Doku
- Extraktion der Daten und neuimplementierung auf aktueller OS/Modulversionen
- Wartung
- Technikeinsatz:
  Ubuntu, später Debian (Linux, PHP)
  Apache, später nginx
  Git
  PHP/MySQL/MariaDB Stack
  Docker
  Lizenzierung und Governance
  FOSS-Software
  Wordpress, Odoo, Ecommerce Anbindung

12/2015 – 08/2019
03/2020 - heute

Externes IT-Management / IT-Architekt; Food-Bereich (P)

- Übernahme der internen IT-Verwaltung von Stunde 0
- Kooperation mit Systempartner aus NRW, nachgelagerte direkte Berichterstattung an GF, implizit gesharter CIO / CISO, Support u.a per Ticketsystem
- Gemeinsame Budgetverantwortung
- Aufnahme IST-Situation/Erarbeitung Soll-Definition
- Entwicklung einer IT-Infrastruktur innerhalb vier Werktagen und Release des Go-Live inkl. Lieferung und Einbau über die Weihnachtsfeiertage bis zum 7.01.2016 für den Start der Tätigkeit mit 20 Personen, größtenteils Remote.
- Umsetzung Terminalserverfunktionen

- Entwicklung und Umsetzung IT-Sicherheitsrichtlinie
- Umsetzung neuer IT-Struktur mit getrennten Netzwerkabschnitten, mittlerweile VLANs
- Einbindung werbewirksames Gästenetzwerk inkl. Trennung vom Internen Netzwerk über zwei Standorte
- Loadbalancing
- Unterrichtung und Planung auf Basis BDSG, DSGVO, BSI-Grundschutz
- Nachgelagerte Schnittstellenfunktionalität/Sourcing und Evaluation
- Mitarbeiterschulung
- Vereinheitlichung Sicherheitsinfrastruktur, Netzwerk und Systemhärtung
- Rollout Eset Server/Client AV
- Erarbeitung Projekte für Kunden des Kunden
- Einsatz neuer, mehrstufiger Methoden zur Einbruchsprävention
- Technikeinsatz:
  Dell Server, Dell Clients
  Sophos SG Firewall
  HPE Switches
  Microsoft AD 2012R2
  Microsoft Exchange 2016
  Microsoft 365, Teams
  Mailarchivierung, Mailverschlüsselung, Prozesseinbindung
  Microsoft Hyper-V 2012R2 / 2016 / 2019
  Microsoft IIS (Internet Information Services) 2012-2019
  Microsoft SQL Server, DBA, Datenbankverwaltung
  Hochverfügbarkeit
  Sage DMS; ERP, SuccessFactors
  Microsoft Terminal-Services Cluster unter 2012R2 / 2019
  Debian Linux (ab V8. Bis aktuelle Version), Ubuntu
  VoIP-TK
  Zammad, elasticsearch,...
  QNAP/Synology NAS
  Backup: Veeam
  Systemmonitoring mit Hilfe des check_mk Stacks
  Dienste: DFS, DNS, DHCP, TCP/IP, Subnetting, Firewalling, Routing
  IT-Beratung, IT-Sicherheitsanalyse, IT-Architektur, SIEM, PHP, MariaDB, jquery
  Hinweis: Beendigung der Zusammenarbeit da Versuch des Aufbaus von lokalen Kompetenzen bzw. Rückgriff auf großes Systemhaus vor Ort, Beginn der Wiederaufnahme der Zusammenarbeit im Q1/2020, Erste größere Projekte im Q3/2020 ff, 2nd und 3rd Level Support
  Lizenzierung und Governance
  FOSS-Software
- Steuerung externer Dienstleister
- Remoteeinsatz: 100%
  Umfang: 60 Mitarbeiter

09/2013 – 08/2017 Externes IT-Management / IT-Architekt; Medienbranche/VA (MAH)

- Aufnahme IST-Situation/Erarbeitung Soll-Definition
- Troubleshooting Instabile und Ineffiziente IT-Struktur
- Entwicklung der neuen IT-Struktur
- Schnittstellenfunktionalität
- technisches Projektmanagement und Organisation in div. Technischen Projekten
- Mitarbeiterschulung
- Budgetverantwortung
- Einsatz neuer, mehrstufiger Methoden zur Einbruchsprävention (digital und Analog)
- Technikeinsatz:
  Dell Server, Dell Clients
  Sophos SG Firewall
  HPE Switches
  FreeNas
  Eset AV
  Microsoft AD 2012R2
  Microsoft Exchange 2013
  Microsoft Hyper-V 2012R2
  Debian/Ubuntu
  FOSS Software
  Licencing and Governance
  Systemmonitoring
  Dienste: DNS, DHCP, TCP/IP, Subnetting, Firewalling, Routing
  IT-Beratung, IT-Sicherheitsanalyse, IT-Architektur
- Steuerung weiterer externer Dienstleister
- Remoteeinsatz: 100%

09/2013 – 11/2013 IT-Restrukteur / Renovator, High-Gastronomie und Hotellerie (B)

- Aufnahme IST-Situation/Erarbeitung Soll-Definition
- Troubleshooting Instabile und Ineffiziente IT-Struktur
- Entwicklung der neuen IT-Struktur
- Schnittstellenfunktionalität
- Mitarbeiterschulung
- Budgetverantwortung
- Einsatz neuer, mehrstufiger Methoden zur Einbruchsprävention (digital und Analog)
- Technikeinsatz:
  HPE / IBM / Dell Server, Dell Clients
  Sophos SG Firewall
  Microsoft AD 2003 / 2008
  Microsoft Terminal-Services Cluster und Hochverfügbare Anbindung der Dienste (Loadbalancing)
  Microsoft Exchange 2013, Mailarchivierung, Mailverschlüsselung
  Backup: Veeam
  Dienste: DNS, DHCP, TCP/IP, Subnetting, Firewalling, Routing
  IT-Beratung, IT-Sicherheitsanalyse, IT-Architektur
- Remoteeinsatz: 100%

darüber hinaus

Tiefe und Breite Kenntnisse in TCP/IP, Telekommunikation/TK, Networking, Firewalling, Open-Source-Software (div), Branchensoftware (div), SQL, breites Virtualisierungs- und Konzeptwissen.
Breite Palette an Hardware, Sicherheitsequipment und Firewall/UTM-Herstellern, Antivirensoftware, Troubleshooting (2nd, 3rd Level…).
Interdisziplinäre Lösungssuche, Automatisierung, seit 2023 verstärkt KI und KI-Implementierung in Geschäftsprozesse

Technisch: Shopsysteme, Learningtools (E-Learning), CRM, CMS,…

Analytical (other) skills: Go-To-Market-Analyse, Vorgehensweisen im Marketing, Interkulturelle Kommunikation.

social Skills: Präsentationen (DE/EN) abgestimmt auf Audienz, Mitarbeiter-, Team- und Projektführung, Konfliktlösung (technisch/sozial), Mediation, Zusammenführen von Interessensgruppen