QUBES PROFIL MICHAEL GEIß

KURZPRÄSENTATION

Michael Geiß (28) ist ein IT-Security Engineer, der sich mit seinen breit aufgestellten Kompetenzen in neuen Situationen stets sicher und sehr gut zurechtfindet. Herausforderungen erledigt er selbstständig mit äußerster Sorgfalt und größter Genauigkeit. Seine fundierten Fachkenntnisse der IT Infrastruktur, die er durch Schulungen stetig erweitert und zertifizieren lässt, setzt er zur Bewältigung verschiedenster Problemstellungen zielführend ein.
Seine Schwerpunkte liegen besonders im Bereich der Administration und Härtung von Windows Systemen, der Virtualisierung, des Netzwerk-Designs und dem Aufbau von IT-Dokumentationen.

Als IT-Consultant teilt er seine Erfahrungen und sein Wissen uneingeschränkt, um den Auftraggebern einen echten Mehrwert zu schaffen. Stets qualitative Arbeitsergebnisse mit entsprechender Kundenabstimmung sorgen für eine zielgerichtete Lösungsorientierung und letztendlich zum Erfolg der aufgetragenen Problemstellungen.

8 JAHRE BERUFSERFAHRUNG

SYSTEM ADMINISTRATOR / SYSTEM ENGINEER
SECURITY ENGINEER
INFORMATIONSSICHERHEITSBEAUFTRAGTER
NETWORK SPECIALIST
PROJECT MANAGEMENT
TESTING

UNTERNEHMENSBRANCHEN

Öffentlicher Dienst
Kommunale- und staatliche Einrichtungen
Logistik
Gesundheitswesen
Consulting

HARD SKILLS

Windows Betriebssysteme 5*
Virtualisierung 4*
Backup 3*
Netzwerk Design 4*
Testmanagement 4*
Linux 3*
System Monitoring 4*
Techn. Projektmanagement 4*
ITSCM, BCM 4*

SOFT SKILLS

Teamfähigkeit 5*
Kunden- und Lösungsorientiertes Arbeiten 5*
Zuverlässigkeit / Verantwortungsbereitschaft 5*
Belastbarkeit 5*
Analytisches Denken 4*
Interne und externe Kommunikation 5*
Entscheidung und Problemlösung 4*

FACHKENNTNISSE / SCHWERPUNKTE

SERVER INFRASTRUKTUR 4*

Server-Hardware (Fujitsu, DELL, HP) VMWare ESXi, vCenter/vSphere (5.x/6.x/7.x), VMWare Workstation (12.x bis 15.x), Oracle VM Virtualbox, Microsoft Hyper-V (2012 bis 2019), Citrix XEN, Citrix NetScaler, Citrix XenDesktop, Citrix XenApp, Microsoft Windows Client (XP, 7, 8, 8.1, 10, 11) Server (2003, 2008, 2008R2, 2012, 2012R2, 2016, 2019,2022), Linux Mint, Ubuntu, SLES, CentOS, MacOS, KaliLinux, ParrotOS

SERVER APPLIKATIONEN 4*

Microsoft: Active Directory (AD), LDAP, Application Server, DHCP Server, Domain Name System (DNS) Server, File Server, WebServer (IIS) Network Policy, Print Server, Remote Access Server, Remote Desktop Services (RDP), WSUS, Group Policy Management, WDS, KMS-Server

NETZWERK 4*

Switch-Hardware, Cisco, HP, diverse Netzwerk-Topologien in Kupfer sowie LWL Verkabelung, OpenVPN, PiVPN, LAN, WAN, WLAN Indoor, QoS, VoIP (AVAYA), Firewalls, Cisco, Juniper Networks, TFK Schulrouter, Gateprotect, Monitoring (PRTG Paessler), NAC, Nessus, Tenable.sc, OPNsense

ANWENDUNGSTOOLS 4*

Microsoft Office (2007 bis 2019), Visio, Project, Outlook, OneNote, Nano, SSH, VMWare, OTRS, i-doit, Docusnap, Putty, Kaspersky Endpoint for Business, Trend Micro Endpoint Security, GData, Cordaware, Project Libre, ISIS12-Software, BSI IT-Grundschutz, Jira, Checkmk, Netbox, Nucleus, YubiKey, RoyalTS (RDP Manager), Wireshark, nmap, Metasploit, hydra

CMS 3*

Joomla, MediaWiki, Confluence (Atlassian)

DATENBANKEN 2*

MySQL, SAP HANA, Oracle DB

PROGRAMMIERUNG 3*

Windows Shell, HTML, PowerShell

PROJEKTE (A=Architect, S=Security, E=Engineer)

05/2022 bis heute | Monate | AS
Qubes GmbH
Kunde: HZD | Wiesbaden | Teilprojektleiter
HessenPC 5.0 auf Grundlage von Microsoft Windows 11 Enterprise

Projektbeschreibung (allgemein):
Der HessenPC basiert auf Windows 10 und Office 2016. Er wurde für die landesweite (Land Hessen) Standardisierung und Harmonisierung geschaffen und seitdem fortlaufend weiterentwickelt. Der HessenPC ist DIE Standard-Anwendungsplattform der Landesverwaltung. Mit dem HessenPC 5.0 stand nun die nächste Herausforderung an. Ziel des Projektes ist die Weiterentwicklung des HessenPC auf Grundlage von Windows 11 und Office 2021 / O365 Apps for Enterprise.

Aufgaben/Tätigkeiten:
- Exakte Definition des zukünftigen HessenPC Standard, mit folgenden Schwerpunkten:
  - Identifikation von nutzbringenden neuen Windows-Funktionen
  - Überprüfung der Datenabflusskontrolle
  - Prüfung neuer Sicherheits Features (OnPrem/Cloud)
- Anfertigung der notwendigen Dokumentationen (GPOs, Architektur, Sicherheitskonzept)
- Dokumentation der technischen Spezifikationen und Freigabe durch die landesweiten Gremien
- Einsparmöglichkeiten identifizieren mit den Schwerpunkten:
  - Vereinfachung bei Sicherheits-Komponenten
  - Reduzierung von Softwarepaketen der neu zu paketierenden Anwendungen
- Fachliche und organisatorische Steuerung des Teams (2 IT-Techniker und 1 IT-Architekt)
- Enge Zusammenarbeit mit Gesamtprojektleitung und Vorbereitung der Status-Berichte für Management
- Zusammenarbeit mit einzelnen Bereichen steuern, die Services für den HessenPC anbieten

Benefits:
- Vorbereitung für eine sichere, hybride Arbeitswelt
- Grundlage für Microsoft Azure Cloud Themenvielfalt geschaffen
- Neue Verwaltung der Fesplattenverschlüsselung
- Einhalten der Microsoft Supportzeiträume (Windows 10 EOL 10/2025)

Schwerpunkte / Kenntnisse
- technische Hands-On Erfahrung
- Steuerung / Planung des HessenPC Designs
- Systemhärtung per Gruppenrichtlinien
- Analyse einzelner Microsoft Azure Komponenten
- Erstellung technischer und organisatorischer Dokumentationen
- Telemetriedaten analysieren und Konfigurationen durchführen
- Release-/Patchmanagement

Produkte:
- Microsoft Windows 11 Enterprise
- Microsoft Windows 10 Enterprise
- MECM
- MS Powershell Scripting
- Microsoft Hyper-V
- Microsoft Gruppenrichtlinien
- BSI IT Grundschutz
- CIS Benchmarks
- DISA STIGS
- Security Baselines Microsoft
- Windows Hello For Business
- Azure AD Anbindung
- Windows 11 Widgets
- Enterprise State Roaming
- Cloud Management Gateway
- Microsoft Endpoint Manager
- Microsoft WSUS

02/2021 bis 04/2022 | 14 Monate | SE
Qubes GmbH
Kunde: HZD | Wiesbaden | Security Engineer
Server Standardisierung Windows Server 2016/2019/2022

Projektbeschreibung (allgemein):
Da in der HZD bisher kein einheitlicher und OE-übergreifender Standard für Windows Server existiert, wurde im Rahmen des Programms 24/7 das Projekt Server Standardisierung initiiert. Ziel des Projektes war die Bereitstellung einer standardisierten Konfiguration für physische und virtuelle Systeme (ESX/Hyper-V) sowie die Schaffung und Etablierung einheitlicher Betriebsprozesse an zentraler Stelle.

Aufgaben/Tätigkeiten:
- Erstellung operatives Sicherheitskonzept
- Erstellung operatives Berechtigungskonzept
- Härtung der Betriebssysteme inkl. Dokumentation
- Tests der Kompatibilität mit Fachverfahren
- Abstimmung mit Fachabteilungen
- Abstimmungen innerhalb des Projektes
- Abstimmungen mit Microsoft DSE
- Recherche/Abstimmung mit Drittanbietern für Security Lösungen
- Definition des Zugriffs auf die Server
- Abstimmung mit ITSibe der HZD
- Enge Zusammenarbeit mit technischem Projektleiter
- Vorstellung des Produktes in verschiedenen Gremien

Benefits:
- Vereinheitlichung der Server im Land Hessen
- Effizientere Prozesse rund um die Serverlandschaft
- Aufbau/Reorganisation Systembetrieb für Server
- Aktuelle Serverbetriebssysteme nach Microsoft Best Practice

Schwerpunkte / Kenntnisse
- Systemhärtung per Gruppenrichtlinien
- Analyse einzelner Server Komponenten
- Erstellung technischer und organisatorischer Dokumentationen
- Telemetriedaten analysieren und Konfigurationen durchführen
- Server Troubleshooting
- Release-/Patchmanagement

Produkte:
- MS Windows Server 2016 (GUI/Core)
- MS Windows Server 2019 (GUI/Core)
- MS Windows Server 2022 (GUI/Core)
- MS Powershell Scripting
- Microsoft Hyper-V
- Microsoft Gruppenrichtlinien
- BSI IT Grundschutz
- CIS Benchmarks
- DISA STIGS
- Security Baselines Microsoft
- Microsoft PAM
- Admin By Request
- UserLock (Multifaktor)

11/2021 bis 03/2022 | 5 Monate | SE
Qubes GmbH
Kunde: Arztpraxis | Kitzingen | Security Engineer
Austausch Netzwerkinfrastruktur, PCs, Server

Projektbeschreibung (allgemein):
Die in die Jahre gekommene Hardware der einzelnen Arbeitsplätze sowie des Servers musste gegen neuere, leistungsfähigere Hardware getauscht und konfiguriert werden. Hierbei galt es die Vorgaben aus TI-Umfeld und vorgeschriebene IT Sicherheitsvorgaben der KVB (Kassenärztliche Vereinigung Bayerns) zu beachten.

Aufgaben/Tätigkeiten:
- Bestandsaufnahme inkl. Erstellung einer Dokumentation
- Zusammenstellung notwendiger Hardware
- Zusammenstellung der eingesetzten Softwareprodukte
- Abstimmungen mit den einzelnen Mitarbeitern in Bezug auf wichtige Details bei Rechnertausch
- Rollout der neuen Hardware und Umzug bestehender Daten sowie Konfigurationen
- Aktualisierung der Praxissoftware TurboMed
- Domänenumzug inkl. Best Practice Security (z.B. LAPS für lok. Admin)
- Zusammenarbeit/Abstimmung mit den einzelnen Dienstleistern (Medizintechnik, Kardiologie, Labor)

Benefits:
- Technologiesprung der Hardware sorgt für deutlich bessere Zugriffszeiten und Performance der Anwendungen
- Beschleunigung der Quartalsupdates von Turbomed (vorher 5h, nach Umstellung 2h)
- Allgemeines Sicherheitsniveau an notwendige Anforderungen angepasst/angehoben

Schwerpunkte / Kenntnisse
- Systemhärtung per Gruppenrichtlinien
- Analyse einzelner Server Komponenten
- Domänenumzug von 2003 auf 2016
- Server Troubleshooting
- Analyse Active Directory
- Software Updates

Produkte:
- MS Windows 10 Pro (64bit)
- MS Windows Server 2003 (GUI)
- MS Windows Server 2019 (GUI)
- Microsoft Gruppenrichtlinien
- BSI IT Grundschutz
- Security Baselines Microsoft
- Microsoft Laps
- David
- TurboMed
- PingCastle
- nmap
- Cisco Switch
- Endian Firewall

11/2020 bis 01/2021| 2,5 Monate | SE
Qubes GmbH
Kunde: matrix AG | München | Security Engineer
Wiederherstellung/Neuaufbau Microsoft Windows Server + Infrastruktur

Projektbeschreibung (allgemein):
Für den Kunden der matrix AG musste nach einem Trojaner-Befall die komplette Infrastruktur neu aufgebaut und wiederhergestellt werden. Hierbei ging es um verschiedene Themen sowohl aus der Microsoft-Welt als auch aus dem Netzwerkbereich. Der Schwerpunkt des Projektes lag auf der Umsetzung der neuen Netzwerkarchitektur. Diese erforderte tiefgreifendes Know How und viel “Best Practice” Erfahrung, da hier viele Probleme mit der isolierten Umgebung aufgetreten sind.

Aufgaben/Tätigkeiten:
• Installation/Konfiguration/Anpassung der DevOps VMs für diverse Einsatzszenarien
• Aufbau Hyper-V Hosts (HP ProLiant) + Grundinstallation
• Steuerung der Anforderungen für die Entwickler Umgebung
• Unterstützung beim Ausrollen der weiteren Standorte (Nürnberg, Rumänien, Kirchentellinsfurt)
• Steuerung/Umsetzung Netzwerk ToDo´s (Austausch Switch-Infrastruktur; Umzug Unifi WLAN Hardware; Troubleshooting)

Benefits:
• Wiederherstellung der Arbeitsfähigkeit
• Aufbau sicherer Netzwerksegmente mit entsprechenden Trennungen
• Modernisierung der Serverbetriebssysteme und der eingesetzten Technologien
• Austausch veralteter Netzwerk- und Serverhardware

Schwerpunkte / Kenntnisse
• IT Dokumentation
• IT Prozesse
• IT Infrastruktur
• IT Security
• Windows
• Infrastruktur/Neuaufbau

Produkte:
• MS Windows Server 2016
• MS Windows Server 2019
• MS Powershell Scripting
• Microsoft Hyper-V
• Windows 10 Enterprise
• Fortinet FortiGate
• Cisco / Huawei Switche
• Wireshark
• nmap
• Ubiquiti UniFi WLAN
• Acronis Cyber Backup

10/2019 bis 08/2020| 11 Monate | SE
Qubes GmbH
Kunde: Brainloop AG | München | Security Engineer
Aufbau Security-Netzwerk + Erhöhung IT-Sicherheit + Aufbau IT-Dokumentationslandschaft

Projektbeschreibung (allgemein):
Es wurde ein umfassendes IT- und Produktions-Redesign der Infrastruktur durchgeführt. Die Durchführung fand in kleineren Projektteams statt. Ziel des Redesigns war die bestehende Sicherheit zu erhöhen und eine weitere Zwischenschicht für die relevanten Produkt-Umgebungen aufzubauen. Die Zwischenschicht wurde als hochsicheres Windows-Server Netzwerk nach Vorgaben der DCSO aufgebaut. Die komplette Active Directory Struktur der Produktivumgebungen musste umgebaut und nach Vorgaben eines Admin Tiering Modells neu konzipiert, getestet und umgesetzt werden.

Aufgaben/Tätigkeiten:
- Implementierung der Sicherheitstools und -Prozesse in die Infrastruktur
- Installation/Konfiguration/Härtung von Windows und Linux Servern nach Vorgaben CIS Benchmark
- Definition von Sicherheitsprozessen
- Erstellung und Erweiterung der Dokumentationen von Infrastruktur und Prozessen
- Etablierung Schwachstellenmanagement und Prozessdefinitionen
- Erstellung von Architekturdokumenten
- Admin Tiering (Konzeption, Umsetzung)

Benefits:
- Absicherung der Produktivumgebung
- Vorbereitung für Audit der DCSO
- Vorbereitungen ISO 27001 & BSI C5 Auditierung
- Ausweitung auf gesamte Firmen-Infrastruktur

Schwerpunkte / Kenntnisse
- IT Dokumentation
- IT Prozesse
- IT Infrastruktur
- IT Security
- Windows / Linux
- Vulnerability Management

Produkte:
- MS Windows Server 2012R2
- MS Windows Server 2016
- MS Windows Server 2019
- MS Word 2016
- MS Excel 2016
- MS Powershell Scripting
- CheckMK
- Trend Micro
- Jira
- Confluence
- OPNsense
- Windows 10 Enterprise
- CentOS 7
- YubiKey
- Nessus
- macOS
- Tenable.sc
- Nucleus
- DocuSnap
- Netbox
- WSUS
- VMware vSphere
- RoyalTS (RDP Manager)

2020 | 2 Monate | E
Qubes GmbH
KUNDE: Brainloop
PROJEKT: CIS-Serverhärtung

Projektbeschreibung:
Härtung der vorhandenen Windows und Linux Server nach Standards der CIS (Center for Internet Security) mit entsprechenden Gruppenrichtlinien. Diese Gruppenrichtlinien wurden als Vorlagen für die einzelnen Server erstellt und dokumentiert. Eine weiterführende Dokumentation mit den Abweichungen zu den Standards der CIS spiegeln die Härtung der einzelnen Umgebungen transparent und sind eine sinnvolle Unterstützung für jegliche Auditierung

Aufgaben/Tätigkeiten:
- Erstellung “Hardening Concept”
- Aufbau der Gruppenrichtlinien für die einzelnen Benchmarks der CIS
- Verantwortung für die komplette Umsetzung in den einzelnen Umgebungen der Firma
- Prüfung der Compliance mit Nessus Professional
- Erstellung einer Übersicht der begründeten Abweichungen

Benefits:
- Verringerung der Angriffsflächen
- Deutlich verbesserte Systemsicherheit
- Vereinfachte Einhaltung und Überprüfbarkeit
- Firmenstandard für gehärtete Server

Schwerpunkte / Kenntnisse:
- Dokumentation
- Gruppenrichtlinien
- umfassendes Windows Server KnowHow

Produkte:
- Windows Server 2012R2
- Windows Server 2016
- Windows Server 2019
- Gruppenrichtlinien
- Nessus Professional
- Microsoft Excel
- CIS Audit Files

2020 | 1 Monat| E
Qubes GmbH
KUNDE: Brainloop
PROJEKT: Aufbau Server-Monitoring

Projektbeschreibung:
Eine ständige Verfügbarkeit der IT-Systeme ist heute in jedem Unternehmen Pflicht. Um diese zu gewährleisten sind Server-Monitoring-Programme unerlässlich. Hierfür wurde für das Security Netzwerk mithilfe der Software CheckMK eine von Grund auf neue Monitoring-Lösung aufgebaut, eingerichtet und an die Bedürfnisse der Umgebung angepasst. Damit können die kritischen Systeme in dieser Infrastruktur 24/7 überwacht und Auffälligkeiten an die entsprechend Verantwortlichen gesendet werden.

Aufgaben/Tätigkeiten:
- Installation/Konfiguration CentOS7 + CheckMK
- Definition der notwendigen Plugins + Server
- Benachrichtigungs- und Alarmierungsketten

Schwerpunkte / Kenntnisse:
- Linux Server Administration
- Konzeption u. Umsetzung

Produkte:
- CheckMK
- CentOS 7
- vSphere

Benefits:
• Kontinuierliche 24/7 Überwachung der Server
• Benachrichtigung bei Auffälligkeiten
• Sicherstellung der Verfügbarkeit

2020 | 5 Monate | E
Qubes GmbH
KUNDE: Brainloop
PROJEKT: Vulnerability Management Program

Projektbeschreibung:
Aufbau eines Schwachstellen Managements für das gesamte Unternehmen. Unterstützung von der Konzeption bis hin zur Verwirklichung der einzelnen Schritte. Aufgebaut wurde das Schwachstellenmanagement für alle Windows und Linux-Systeme. Hierbei wurde mithilfe von Nessus Professional und Tenable.sc das Management der Vulnerabilites verwirklicht und mit Jira die Schwachstellenbehebung verfolgt. Unterteilt läuft das VMP nun in drei Phasen ab (Assessment, Management, Remediation)

Aufgaben/Tätigkeiten:
• Installation/Konfiguration der Tools Nessus Professional und Tenable.sc
• Unterstützung bei der Konzeption des Vulnerability Management Programs
• Behebung der Schwachstellen im Security Network
• Unterstützung der einzelnen Abteilungen bei der Schwachstellenbehebung und Dokumentation
• Aufbau einer Knowledge Base der behobenen Schwachstellen

Benefits:
• Steigerung der Unternehmenssicherheit
• Übersicht der Risiken und welche zu beheben sind
• Bekannte Sicherheitslücken aufdecken, bevor Angreifer sie finden.
• Unterstützung für eine geschäftliche Risiko-/Nutzen-Kurve und die Optimierung von Sicherheitsinvestitionen.

Schwerpunkte / Kenntnisse:
• Umfassende Kenntnisse Schwachstellenmanagement
• Projektleitung
• Umsetzungen der Maßnahmen

Produkte:
• Tenable.sc
• Nessus Professional
• CentOS 7
• Microsoft Windows Server 2012R2
• Microsoft Windows Server 2016
• Microsoft Windows Server 2019
• Microsoft Word u. Excel

2019 | 1 Monat | E
Qubes GmbH
KUNDE: Brainloop |
PROJEKT: Role Based Access Control (RBAC)

Projektbeschreibung:
Im Zuge der langfristigen Einführung eines zentralen IAM-Systems wurden für die die einzelnen Umgebungen nun Rechte- und Rollenkonzepte analysiert, erstellt und ausgerollt

Aufgaben/Tätigkeiten:
- Mitwirkung bei der Konzeption und Umsetzung der RBAC-Konzepte
- Unterstützung der Fachabteilungen bei Umsetzungsschwierigkeiten
- Für Security Network und Produktivumgebung: Erstellung eines Admin Tiering Konzepts

Benefits:
- Verbesserung der betrieblichen Effizienz
- Verringerung des Risikos von Sicherheitsverletzungen und Datenverlusten/-abzügen
- Verbesserung der Compliance

Schwerpunkte / Kenntnisse:
- Konzeption/Design
- Planung Umsetzung
- Zeitplanung

Produkte:
- Microsoft Active Directory
- Microsoft Admin Tiering

2019 | 1 Monat | E
Qubes GmbH
KUNDE: Brainloop |
PROJEKT: Aufbau IT-Dokumentation und Asset-Management

Projektbeschreibung:
In der IT veralten Dokumente, Anweisungen und Installationsanleitungen sehr schnell. Ziel ist gewesen, eine Dokumentation aufzubauen die sich auch langfristig auf aktuellem Stand halten lässt. Zudem ist eine saubere Dokumentationslandschaft für jegliche Auditierung eine sinnvolle und einfache Unterstützung.

Aufgaben/Tätigkeiten:
- Aktualisierung der vorhandenen Dokumente im Intranet
- Aufbau der kompletten Security Network Dokumentation
- Erstellung einer Technical Knowledge Base, Troubleshooting, Handbüchern und Installations Guides
- Installation/Konfiguration DocuSnap
- Erstellung von Reports und automatisierten Tasks in DocuSnap

Benefits:
- Übersicht aller unternehmensweiten Assets
- Verbesserung der Compliance und Vereinfachung von Auditierungen durch ausführlichen Dokumentationsstand
- Erhöhung der Transparenz des gesamten Security Networks

Schwerpunkte / Kenntnisse:
- Konzeption
- Umsetzung
- Troubleshooting
- Automatisierte Asseterfassung

Produkte:
- Confluence (Intranet)
- Jira
- DocuSnap
- Microsoft SQL
- Windows Server 2019

2020 | gesamte Projektlaufzeit 11 Monate | E
Qubes GmbH
KUNDE: Brainloop
PROJEKT: Troubleshooting und Maintenance Security Network

Projektbeschreibung:
Übernahme der Verantwortung für das Security Network (21 Windows und Linux Server), welches als “Einstiegspunkt” für alle Produktivumgebungen genutzt wird. Hier fallen tägliche Wartungsarbeiten der unterschiedlichen Applikationen als auch der Server selbst an. Diese Arbeiten müssen sowohl durchgeführt als auch dokumentiert werden.

Aufgaben/Tätigkeiten:
• Durchführung von Updateläufen, Upgrades und Systemanpassungen
• Verbesserung der einzelnen Konfigurationen der Systeme
• Pflege des WSUS und aller Applikationen (Trend Micro, Nessus, Tenable.sc, Contechnet, DocuSnap)

Benefits:
• Sicherstellung einer reibungslosen Verfügbarkeit der Umgebung
• Aufrechterhaltung eines festgelegten Sicherheitsstandards und einer entsprechenden Systempflege
• Lückenlose Dokumentation von Problemen und Wartungsarbeiten

Schwerpunkte / Kenntnisse:
• Wartung der kompletten Umgebung
• Troubleshooting
• Benutzersupport
• Umsetzung neuer Anforderungen
• Konfigurationen laut Sicherheitskonzept

Produkte:
• Royal TS
• Microsoft Windows Server 2016
• Microsoft Windows Server 2019
• Microsoft SQL
• Microsoft Powershell

2019 | 1 Monat | E
Qubes GmbH
KUNDE: Brainloop
PROJEKT: Security Information and Event Management (SIEM)

Projektbeschreibung:
Unterstützung bei der Konzeption und Einrichtung eines SIEM-Systems mithilfe des ELK-Stacks. Definition der Alarmmeldungen und Auswertung der Windows-Event IDs für Benachrichtigung.

Aufgaben/Tätigkeiten:
• Mitwirkung bei der Konzeption
• Definition für das Security Network anhand festgelegter Anwendungsbeispiele
• Unterstützung des Logging&Monitoring Teams beim Ausrollen der Komponenten und der Konfiguration

Benefits:
• Daten-Aggregation
• Daten-Normalisierung
• Einhaltung der Compliance
• Bedrohungserkennung und Sicherheitsalarmierung

Schwerpunkte / Kenntnisse:
• Unterstützung/Design
• Zeitplanung
• Umsetzung der Konfigurationen
• Auswertung Windows Event Logs

Produkte:
• ELK Stack
• Audibeat
• Heartbeat
• Winlogbeat
• Gruppenrichtlinien
• Windows Event Logs

2019 | 4 Monate | E
Qubes GmbH
KUNDE: CGM | Koblenz | System Engineer
PROJEKT: Monitoring und Ticketbearbeitung für die Telemed-Infrastruktur

Projektbeschreibung:
Ziel des Projektes war die Übernahme der Schichtdienste im Monitoring und Ticketing sowie die Übernahme kleinerer Projekte zur Verbesserung der Infrastruktur (Reportingserver, Systemdokumentation, Anpassungen bestehende Infrastruktur).

Aufgaben/Tätigkeiten:
- Konfiguration und Monitoring
- Konfiguration einzelner Netzwerkkomponenten
- Störungsanalyse, -bewertung, -überwachung, -behebung
- Aufbau von SQL-Reportingserver
- Dokumentation der durchgeführten Arbeiten

Benefits:
- Instandhaltung der Systeme
- Aufrechterhaltung des Schichtbetriebs
- Erweiterung Dokumentationsumfang

Schwerpunkte / Kenntnisse:
- Monitoring / Störanalyse
- Ticketbearbeitung
- Dokumentation

Produkte:
- Checkmk
- Ubuntu / CentOS
- Windows Server 2016
- Jira
- Confluence
- MSSQL 2016
- VMWare vSphere
- Netbox

2019 | 1 Monat (Kurzprojekt) | E
Qubes GmbH
KUNDE: Accenture | vertraulicher Ort | IT-Consultant Client Engineering
PROJEKT: Technische Umsetzung der Anforderung im Umfeld von Windows 10 LTSC 1809 Image Design & SAC 1809

Projektbeschreibung:
Ziel des Projektes ist die Optimierung von Sicherheitsverbesserungen für Bedrohungsschutz, Informationsschutz sowie die Implementierung von SCCM + USB

Aufgaben/Tätigkeiten:
- Analyse der aktuellen Group Policy Objekte (GPOs)
- Machbarkeits- und Risikoeinschätzung bzgl. der geforderten (GPL) GPOs und Einstellungen
- Reporting der GPOs und des Clientdesigns an den Kunden und die Gesamtprojektleitung
- Analyse der Key Änderungen-Client Implementierung und Deploymentvorbereitung (SCCM + USB)
- Client Test und Pilotierung

Benefits:
- Saubere Einschränkung der Win10-Clients
- Separierung der Win10-Clients in ADS
- Erhöhung der Betriebssicherheit in der Behörde

Schwerpunkte / Kenntnisse:
- IT Infrastruktur / Security
- Client Engineering
- GPL / GPOs

Produkte:
- Windows 10 1809
- SCCM CB 1810
- Windows Server 2016

2018 | 23 Monate | AS
Landratsamt Kitzingen | Kitzingen | Informationssicherheitsbeauftragter
PROJEKT: Einführung ISMS und Strukturierung IT-Dokumentation

Projektbeschreibung:
Die Digitalisierung vieler Funktionen im Landratsamt stellen steigende Sicherheitsanforderungen an die IT-Systemlandschaft. Ziel war die vollständige Dokumentation dieser Landschaft und die Umsetzung des ISMS.

Aufgaben/Tätigkeiten:
- Erstellung der Leitlinie für Informationssicherheit
- Erarbeitung und Erweitern des Informationssicherheitskonzepts
- Konzepterstellung Informationssicherheit
- Koordination zwischen den Abteilungen
- Koordination von zielgruppenorientierten Sensibilisierungs- und Schulungsmaßnahmen

Benefits:
- Framework für die Sicherheit der Informationen
- Richtlinien und Verfahren um Vertraulichkeit, Verfügbarkeit und Integrität von Informationen zu schützen
- Ganzheitlicher Ansatz umfasst die gesamte Organisation

Schwerpunkte / Kenntnisse:
- ISMS
- Koordination der umzusetzenden Maßnahmen
- Interne und externe Kommunikation
- Synergien mit dem Datenschutz
- Verwaltungsmaßnahmen / Verwaltungsabläufe

Produkte:
- ISIS12-Software
- BSI IT-Grundschutz
- Microsoft Visio
- Microsoft Office
- Microsoft PowerPoint
- DocuSnap

2017 | 8 Monate | AS
Landratsamt Würzburg | Würzburg | Informationssicherheitsbeauftragter
PROJEKT: Startschuss / Planung Informationssicherheitsmanagement

Projektbeschreibung:
Die Gesetzeslage verpflichtet die öffentlichen Stellen bis zu einem Stichtag ein Informationssicherheits-Managementsystem einzuführen. Ziel des Projekts war der Vergleich verschiedener Standards (VdS10.000, ISIS12, BSI-Grundschutz) auf Anwendbarkeit in der Verwaltung.

Aufgaben/Tätigkeiten:
- Mitwirkung bei der Kommunikation im Landratsamt
- Erstellung einer Umsetzungsliste
- Priorisierung der erforderlichen Schritte, auch abteilungsübergreifend
- Mehrere Fachvorträge vor verschiedenen Gremien
- Kommunikation mit der Führungsebene

Benefits:
- Sensibilisierung Behördenleitung und Führungskräfte für das Themengebiet
- Zielsetzung der Fachbereiche für die Umsetzungsphase
- Einbindung der gesamten Verwaltung in den ISMS-Prozess

Schwerpunkte / Kenntnisse:
- ISMS
- BSI Grundschutz
- Kommunikationsstärke
- Verwaltung
- Koordination
- Präsentation

Produkte:
- ISIS12-Software
- BSI IT-Grundschutz
- Microsoft Visio
- Microsoft Office
- Microsoft PowerPoint

2017 | 2 Monate | E
WSW Software GmbH | Krailling | System Administrator
PROJEKT: Einführung einer neuen Backup-Lösung

Projektbeschreibung:
Die vorhandene Backup-Software erfüllte nicht mehr die Anforderungen an Verfügbarkeit, Backup-Geschwindigkeit und Wiederherstellung. Um diese Problematik zu lösen, wurde auf den Server-Systemen eine neue Software zur Sicherung eingeführt. Betroffen waren hier vor allem die Datenbank-Server (HANA-DB / Oracle-DB)

Aufgaben/Tätigkeiten:
- Planung des Software-Rollouts
- Abstimmung mit den Datenbankadministratoren
- Verfügbarkeitsanforderungen neu definieren
- Testsituation für die Umgebung erstellt
- Installation und Konfiguration von Veeam Backup & Replication

Benefits:
- Verkürzte Backup- und Restore-Zeiten
- Vereinfachte Übersicht und komprimierte Backup-Jobs
- Backup der SAP-Datenbanken nicht mehr über Umwege

Schwerpunkte / Kenntnisse:
- Netzwerk
- Backup & Storage
- Virtualisierung
- Testing
- Konzeption DB-Jobs

Produkte:
- Microsoft Windows Server 2012R2
- SLES-Linux-Server
- Veeam Backup & Replication
- PowerShell
- SAP HANA
- Oracle DB
- Windows Shell

2017 | 2 Monate | E
WSW Software GmbH | Krailling | System Administrator
PROJEKT: 1st und 2nd Level Support

Projektbeschreibung:
Unterstützung der internen IT im 1st und 2nd Level Support. Richtige Priorisierung der eingehenden Tickets und Weiterleitung an entsprechende Abteilungen. Füllen der FAQ-Datenbank mit neuen Problemstellungen und den damit verbundenen Lösungen.

Aufgaben/Tätigkeiten:
- Koordination der Kommunikation zwischen internen und externen Mitarbeitern
- Ausarbeitung und Erweiterung der FAQ-Datenbank
- Ticketbearbeitung
- Weiterentwicklung und Wartung der Netzwerk- und Security-Infrastruktur

Benefits:
- Entlastung der IT-Mitarbeiter bei Routineaufgaben
- Erweiterung der FAQ-Datenbank mit Support-Wissen
- Schnellere Abwicklung von Standard-Problemen

Schwerpunkte / Kenntnisse:
- Teamkoordination
- Kunden-/ Mitarbeiterabstimmung
- Lösungsorientierung
- Change Management
- Prozessoptimierung

Produkte:
- Microsoft Office
- OTRS
- Confluence
- Microsoft Hyper-V

2016 | 2 Monate | E
Stadtverwaltung Bad Kissingen | Bad Kissingen | System Engineer
PROJEKT: Rollout neuer Drucker für die gesamte Stadtverwaltung

Projektbeschreibung:
Die Leasingverträge der Altgeräte waren ausgelaufen, damit verbunden auch entsprechende Wartungs-/Supportverträge mit dem Hersteller. Aus diesem Grund wurden neue Geräte angeschafft, die innerhalb kürzester Zeit an den einzelnen Standorten getauscht werden mussten.

Aufgaben/Tätigkeiten:
- Erstellung der Umsetzungsplanung
- Erstellung Terminplan
- Vorbereitungen für reibungslosen Tausch der Geräte
- Aktualisierung der IP-Adressen und Funktionseinstellungen
- Einrichtungen auf dem Printserver
- Anpassungen an den Arbeitsplätzen der Mitarbeiter

Benefits:
- Vereinfachter Administrationsaufwand durch vereinheitlichte Geräte
- Geringere Wartungskosten
- Einfacheres Drucker-Handling

Schwerpunkte / Kenntnisse:
- Dokumentation
- Zeitmanagement
- Koordination der Abteilungen
- Kommunikation

Produkte:
- Kyocera Drucker
- Windows Printserver
- Microsoft Visio
- Microsoft Office
- Windows Shell / Scripting

2016 | 3 Monate | E
Stadtverwaltung Bad Kissingen | Bad Kissingen | System Engineer
PROJEKT: Anpassungen an den PC-Arbeitsplätzen für neues Corporate Design

Projektbeschreibung:
Mit der Einführung einer neuen Designstrategie und dem veränderten Auftreten des Erscheinungsbilds mussten auch interne Anpassungen an diversen Vorlagen, Fachverfahren, Arbeitsabläufen angepasst werden.

Aufgaben/Tätigkeiten:
- Teilnahme an Meetings mit externem Dienstleister
- Umsetzung der Vorlagen an den Arbeitsplätzen (ca. 150)
- Möglichkeiten der zentralen Verteilung geprüft, konzipiert, umgesetzt
- regelmäßiges Statusupdate an Behördenleitung
- Kommunikation mit den einzelnen Abteilungen

Benefits:
- Einheitliches Auftreten
- Mitarbeiter müssen sich um Anpassungen nicht selbst kümmern
- Überarbeitete Formulare/Anträge

Schwerpunkte / Kenntnisse:
- Testkonzeption
- Microsoft Word Makros
- Microsoft Outlook Signaturverwaltung
- Kommunikation (intern/extern)

Produkte:
- Microsoft Office
- Microsoft Windows 7
- Microsoft Server ADS/Group
- HTML

2016 | 2 Monate | S
Stadtverwaltung Bad Kissingen | Bad Kissingen | Project Management
PROJEKT: Einführung einer Alarmierungslösung

Projektbeschreibung:
Für die PC-Arbeitsplätze in der Stadtverwaltung wurde eine Alarmierungslösung gewünscht. Mit der angeschafften Software (Cordaware) sollte es den Mitarbeitern möglich sein bei Bedarf Kollegen, die bei einem Notfall unterstützen können, zu alarmieren.

Aufgaben/Tätigkeiten:
- Konzepterstellung mit den Verantwortlichen
- Software-Auswahl mit Test verschiedener Lösungen
- Anpassungen der Software an die Gegebenheiten
- Testszenarien an vorher definierten Arbeitsplätzen
- Rollout auf die PC-Arbeitsplätze

Benefits:
- Erweiterung des Sicherheitskonzepts
- Einfache Notruf-Lösung
- Einfache Skalierbarkeit

Schwerpunkte / Kenntnisse:
- Problemlösungskompetenz
- Kommunikationsstärke
- Dokumentation
- Planung und Design

Produkte:
- Cordaware
- Microsoft Windows
- Microsoft ADS/DNS
- Windows Shell
- GPOs zum Ausrollen des Clients

2016 | 3 Monate | AE
Stadtverwaltung Bad Kissingen | Bad Kissingen | Project Management
PROJEKT: Einführung IT-Dokumentation

Projektbeschreibung:
Dezentrale Ansammlung von Dokumenten, FAQs und sonstigen angesammelten Wissensdaten sollten an einer zentralen Stelle zusammenlaufen und von dort aus abrufbar sein.
Ziel: Vereinheitlichung und Komprimierung des IT-Wissens.

Aufgaben/Tätigkeiten:
- Konfliktmanagement
- Vertretung der Interessen der einzelnen IT-Mitarbeiter
- Zuteilung von Dokumentations-Gebieten
- Aufbau eines Dokumentationsstandards
- Einführung der Lösung
- Schulung der Mitarbeiter

Benefits:
- Zentrale Ablage für notwendiges IT-Wissen
- Schnelle Verfügbarkeit, an jedem PC-Arbeitsplatz möglich
- Einfaches Befüllen, durch verschiedene Anpassungen

Schwerpunkte / Kenntnisse:
- Team Koordination & Management
- Dokumentation

Produkte:
- Microsoft Office
- Windows Explorer
- PRTG
- i-doit (CMDB & IT Documentation)

2015 | 5 Monate | E
Stadtverwaltung Bad Kissingen | Bad Kissingen | System Administrator & Testing
PROJEKT: Ablösung veralteter Infrastruktur (Windows Server & Hardware)

Projektbeschreibung:
Ziel dieses Projekts war die Konsolidierung verschiedener Server und Systeme. Herausforderung waren die darauf laufenden Fachverfahren, für die es teilweise keinen Hersteller Support mehr gab.

Aufgaben/Tätigkeiten:
- Aufnahme der veralteten Server-Systeme und Insellösungen
- Abstimmung mit den einzelnen Abteilungen zwecks Abschaltung / Umstellung
- Zeitplanung für die Umstellungen
- Abschaltung und Entsorgung der Altgeräte

Benefits:
- Sicherheitslücken durch veraltete Systeme geschlossen
- Dokumentation des Software-Bestandes
- Bessere Verfügbarkeit der Anwendungen

Schwerpunkte / Kenntnisse:
- Geräteverwaltung
- IT Sicherheit
- Dokumentation
- Prozessoptimierung
- Zeitmanagement

Produkte:
- Windows Server 2000, 2003, 2008
- Microsoft Office
- Microsoft Visio
- Robocopy
- VMWare vSphere

2015 | 4 Monate | E
Stadtverwaltung Bad Kissingen | Bad Kissingen | System Administrator
PROJEKT: Hardware Rollout

Projektbeschreibung:
Ziel des Projekts war die Ablöse der übrigen Windows-XP Rechner. Hier mussten spezifische Softwareprodukte in Zusammenarbeit mit den Herstellern umgezogen werden. Übernahme der Altdaten und Funktionstests mit den jeweiligen Mitarbeitern bildeten den erfolgreichen Abschluss.

Aufgaben/Tätigkeiten:
- Aufnahme der Hardware und Software vor Ort
- Absprache mit den Teamleitern und Facharbeitern
- Erstellung der Zeitplanung für die einzelnen PC-Arbeitsplätze
- Ausarbeitung von Testszenarien

Benefits:
- Leistungsstarke und aktuelle Hardware für die Spezialsoftware
- Sicherheitstechnisch wieder auf aktuellen Stand
- Weniger Ausfälle und gestiegene Verfügbarkeit der Systeme

Schwerpunkte / Kenntnisse:
- Detaillierte Dokumentation
- Zeitmanagement
- Kommunikation mit internen und externen Mitarbeitern
- Federführung für den Projekterfolg
- IT Sicherheit

Produkte:
- AquaInfo
- Windows XP / 7 Prof.
- Aquasys
- BTB
- Videoüberwachung Mobotix
- Microsoft Visio

2015 | 3 Monate | SE
Stadtverwaltung Bad Kissingen | Bad Kissingen | Project Management & Testing
PROJEKT: Einführung neuer Firewall-Lösungen in den Schulen

Projektbeschreibung:
Die über Jahre veralteten Firewall-Lösungen an den betreuten Schulen der Stadtverwaltung Bad Kissingen mussten aus Sicherheitsgründen (keine Updates und Maintenance mehr) getauscht werden. Hierfür sollten drei verschiedene Hersteller miteinander verglichen werden.

Aufgaben/Tätigkeiten:
- Erstellung einer IST-Analyse
- Anfertigung des zukünftigen Firewall-Designs mit Visio
- Ausarbeitung SOLL-Konzept
- Abstimmung mit den IT-Mitarbeitern für die Umsetzungsphasen
- SWOT-Analyse / Vergleich der Lösungen
- Test Integration
- Rollout der vorher konfigurierten Systeme

Benefits:
- Deutliche Steigerung des Sicherheitsniveaus
- Saubere Trennung der vorhandenen Netze
- Vereinfachtes Handling für die Lehrkräfte

Schwerpunkte / Kenntnisse:
- IT Sicherheit
- Funktionstests
- Konzeption
- Dokumentation
- Präsentation der Benefits

Produkte:
- Fortinet Firewall
- Time-for-Kids Schulrouter
- Gateprotect Firewall
- Linux IPFire
- Microsoft Visio
- Microsoft Office
- Microsoft ADS / DHCP / DNS / WSUS

2014 | 2 Monate | AE
Stadtverwaltung Bad Kissingen | Bad Kissingen | System Engineer
PROJEKT: IT-Organisation an den betreuten Schulen

Projektbeschreibung:
Die betreuten Schulen der Stadt Bad Kissingen (Grund- und Mittelschule) wurden hinsichtlich der internen IT-Ausstattung weitestgehend von den Auszubildenden betreut. Hier war der Wunsch des Projekts diese nun durch einen festen Mitarbeiter betreuen zu lassen, um so mehr fachliches Know-how einbringen zu können und die Reaktionszeiten zu minimieren.

Aufgaben/Tätigkeiten:
- IST-Analyse
- Erarbeitung eines SOLL-Konzepts mit den Verantwortlichen
- Vorstellung der angedachten Umsetzung
- Change- und Releasemanagement der betreuten Systeme

Benefits:
- Schnellere Abwicklung zukünftiger Maßnahmen
- Zentraler Ansprechpartner
- Prozessoptimierung
- Homogenisierung der Umgebungen

Schwerpunkte / Kenntnisse:
- Koordination der Betroffenen
- Umsetzung
- Dokumentation

Produkte:
- Microsoft Office
- Microsoft Visio
- Microsoft Hyper-V
- WinSV/ASV
- Mastersolution
- netadmin

2014 | 2 Monate | AE
Stadtverwaltung Bad Kissingen | Bad Kissingen | System Engineer
PROJEKT: Einführung neue Antiviren-Lösung

Projektbeschreibung:
Die bisher vorhandene Lösung Trend Micro Endpoint Security sollte durch Kaspersky Endpoint for Business abgelöst werden.

Aufgaben/Tätigkeiten:
- IST-Analyse
- SOLL-Konzept, Rollout-Planung
- Umsetzung der SOLL-Konzeption
- Sicherstellung eines reibungslosen und störungsfreien Betriebes

Benefits:
- Erweiterung Funktionsumfang
- Erhöhung der Sicherheit der einzelnen Clients
- Zentrale Management-Konsole

Schwerpunkte / Kenntnisse:
- Koordination der Abteilungen
- Migration von Diensten
- Security
- Dokumentation

Produkte:
- Microsoft Office
- Microsoft Visio
- Kaspersky Endpoint for Business
- VMWare vSphere
- Trend Micro Endpoint Security

AUS-UND WEITERBILDUNG

11/2020 bis heute |
TryHackMe (Top 1%)
https://tryhackme.com/p/Crushi

Pentesteracademy
Attacking and Defending Active Directory
Pentesting with Metasploit
Network Pentesting

INE
Junior Penetration Tester

TCM Security
Practical Ethical Hacking
External Pentest Playbook

11/2018 bis 03/2020 | 16 Monate
manQ – Management Qualifizierung (Operativer Professional)
Certified IT Business Manager IHK

07/2017 | 1 Monat
Bayerische Verwaltungsschule
zertifizierter Informationssicherheitsbeauftragter (Theorie und Praxis, Aufgaben eines ISBs, Vorgehensweise im Unternehmen, Aufbau eines ISMS, Vorstellung der Standards: VdS 10 000, ISIS12, BSI IT-Grundschutz, ISO 27001, Kommunikationsmöglichkeiten, Aufbau von Schulungen zur Mitarbeitersensibilisierung, Kategorisierung von IT-Risiken, Schnittmengen mit dem Datenschutz)

11/2015 bis 07/2016 | 8 Monate
Fernschule Weber
Netzwerktechnik (Grundlagen der Netzwerktechnik, Netzwerk-Topologien, ISO/OSI Referenzmodell, Netzwerkkomponenten, Netzwerkprotokolle: TCP/IP, IPv6, UDP, DNS, HTTP, HTTPs, SNMP, DHCP, Konfiguration von Switches und Routern, ISDN, DSL, WLAN, Netzwerkdokumentation, Netzwerk-Management, Netzwerküberwachung, Netzwerk-Sicherheit, Netzwerk-Tools, Troubleshooting, Fehlersuche und -behebung unter Windows-Servern)

11/2014 bis 10/2015 | 11 Monate
Fernschule Weber
IT-Security (Grundlagen der Datenkommunikation, Kryptologie, Access Control, Sicherheitsmodelle, Architekturen und Evaluation, Sicherheitsstandards und Normen, Forensik und Datenrettung, Sicherheitsmanagement und Managementsysteme, Sicherheits- und Risikomanagement, Operations-Sicherheit, Business-Continuity und Disaster-Recovery, Software-Sicherheit, Change Management, Software-Lebenszyklus, Recht und Ethik - Innere Gebäudesicherheit)

09/2013 bis 05/2014 | 8 Monate
Berufsschule Heinrich-Thein
CCNA Exploration: Routing Protocols and Concepts