

Beschreibung der Systemlandschaft

1. Allgemeines

Die WFBB Wirtschaftsförderung Land Brandenburg GmbH (WFBB) nutzt eine MS-Windows basierende EDV-Landschaft. Es wird die aktuellste Systemsoftware genutzt, die durch permanente Updates und Upgrades auf dem neuesten Stand gehalten wird. Neben der Zentrale in Potsdam ist die WFBB im Land Brandenburg an sechs weiteren Standorten vertreten: Neuruppin, Eberswalde, Cottbus, Frankfurt (Oder), Potsdam Friedrich-Engels-Str. und Schönefeld. Die Standorte sind mittels VPN an das LAN der Zentrale angebunden. Die Server der Zentrale sind auf zwei Technikräume verteilt, um Anforderungen hinsichtlich Verfügbarkeit und Sicherheit zu genügen (Backuptrennung von Daten).

Es wird eine hochverfügbare Virtualisierungsumgebung auf Basis von Windows Server 2025 eingesetzt. Nahezu alle zentralen Dienste werden als virtuelle Maschinen ausgeführt.

2. Internetverbindung

Die Zentrale in Potsdam ist über eine 500 Mbit/s Standleitung mit dem Internet verbunden, während die weiteren Standorte über min. 20 Mbit/s Internetverbindungen verfügen.

3. Firewall

Das Netz ist über eine mehrstufige redundante Firewall-Infrastruktur in die Bereiche LAN, Perimeter und WAN unterteilt und abgesichert.

4. Externe Dienste

Den Nutzern werden verschiedene Dienste auch außerhalb des LANs angeboten. Hierzu gehören u.a. Netzzugang per Citrix, Webmailzugriff und Handysynchronisation mittels ActiveSync.

Zusätzlich wird über eine Datenbankverbindung die Webseite der WFBB mit Inhalten gefüllt. Die Gewerbedatenbank, Bestandteil des KWIS.net, wird von den Kreisen mit Daten gefüllt und unter anderem im Internetauftritt der WFBB angezeigt. Ein weiterer Internetauftritt ist das Fachkräfteinformationssystem.

Die veröffentlichten Dienste werden teilweise durch Web Application Firewalls auf der Perimeter-Firewall abgesichert. Weiterhin werden Dienste wie Teams von Office 365 genutzt.

5. Mailsystem

Als Mail- und Groupware wird Microsoft Exchange SE in einer hochverfügbaren Installation eingesetzt. Die Zugriffe werden mittels redundanter Loadbalancer auf die Exchangeserver verteilt. In der DMZ wird ein Exchange SE Server mit der Edge Rolle betrieben, welcher die Spamfilterung durchführt. Die Logs des Spam-Filters werden auf einem separaten Server in eine SQL-Datenbank gespeichert. Für die Exchange Hybridbereitstellung mit Centralized Mailflow wird ein weiterer Exchange Edge Server in der DMZ betrieben.

Die Archivierung der Postfächer erfolgt durch die Archivierungssoftware Mailstore, welche auf einem separaten Server installiert ist. Für die Verschlüsselung und Signatur mittels S/Mime Zertifikaten wird eine Zertificon Z1 SecureMail Gateway Lösung eingesetzt. Diese stellt automatisiert Zertifikate für die internen Nutzer bereit. Für das Monitoring der Mail-Reputation und der Email-Konfiguration in den Bereichen SPF, DKIM und DMARC wird ein cloudbasierter Service genutzt.

6. Datensicherung

Die Datensicherung für alle Bereiche der WFBB erfolgt in der Zentrale in Potsdam. Sicherungen werden sowohl auf Festplatten als auch auf Bändern abgespeichert. Als Backupsoftware wird Veeam B&R verwendet.

7. Anbindung der externen Standorte und Remote Access

Die externen Standorte sind primär über Sophos RED Devices an den Hauptstandort angebunden. Die Internetverbindung erfolgt über regionale Provider. Grundsätzlich erfolgt keine externe Datenhaltung außerhalb der Zentrale.

Für externe Zugriffe auf interne Ressourcen und diverse Spezialanwendungen wird außerdem eine Terminalserver-Farm mit Citrix betrieben, bestehend aus drei Terminalservern. Zugriffe auf die Terminalserver von extern werden über einen Citrix Netscaler ermöglicht.

Als Remote Access VPN wird Microsoft DirectAccess eingesetzt.

Eine Migration von Microsoft DirectAccess zu einer Microsoft Always On VPN Dual-Tunnel-Infrastruktur ist in Planung.

8. Verzeichnisdienst

Als zentraler Verzeichnisdienst wird Active Directory eingesetzt. Alle Benutzer, Computer und Gruppen werden innerhalb des Active Directory verwaltet. Die Rechteverwaltung aller Anwendungen und Dienste erfolgt innerhalb des Active Directory, soweit dieses die Möglichkeit hierzu bieten. Benutzer und Computer werden mit Hilfe von Gruppenrichtlinien zentral administriert.

8.1 Active Directory Federation Services (ADFS)

Redundante Active Directory Federation Services ermöglichen die Authentifizierung verschiedener Cloud Applikationen. Hierzu zählen u.a.:

- Microsoft 365
- Cisco Duo
- Cisco Meraki

9. Clouddienste

Es werden Dienste von Microsoft 365 genutzt. Vorrangig ist dies aktuell Teams. Hierzu existiert ein Tenant, welcher mittels EntraID Connect die Nutzerkonten aus dem lokalen Active Directory erhält. Die Authentifizierung an M365-Diensten erfolgt mittels Active Directory Federation Services.

Cisco Duo stellt die Multifaktor Authentifizierung für die Nutzer bereit. Cisco Meraki wird für die Verwaltung von mobilen Endgeräten genutzt. Weiterhin existieren Konten diverser Newsletterversender, welche in den Mailflow eingebunden wurden.

Aktuell wird eine Migration des MDMs von Cisco Meraki zu Microsoft Intune geplant.

10. Multifaktor Authentifizierung

Anmeldungen bei diversen Diensten wie Cisco Duo und Meraki, Microsoft 365 und Citrix Netscaler sind derzeit mittels der Multifaktorlösung Cisco Duo abgesichert. Weitere Dienste sind für die Absicherung mittels Duos vorgesehen.

11. Zertifizierungsstelle

Für die Absicherung und Authentifizierung interner Verbindungen wird eine zweistufige PKI mit einer Offline Root CA eingesetzt. Die Issuing CAs stellen u.a. die Zertifikate für interne Webdienste, Computerzertifikate für die RDP-Absicherung und Netzwerk-Authentifizierung im LAN- und WLAN bereit.

Außerdem wird eine SCEP-CA zur Ausstellung von Zertifikaten für diverse Nicht-Windows-Geräten eingesetzt.

12. Filesystem

Die Dateien der Nutzer liegen auf einem Windows Server 2025 Fileserver. Die Berechtigungen werden mittels Gruppen aus dem Active Directory gesteuert.

13. Datenbanken

In der WFBB werden hauptsächlich Datenbanken mit Microsoft SQL Server 2025 verwendet. Zu den Diensten, die Datenbanken auf dem Server verwenden, gehören u.a. das Dokumentenmanagementsystem sowie das KWIS.net (Kommunales Wirtschaftsinformationssystem).

14. Infrastruktur

Für das EDV-Netz wird die Infrastruktur des Hauses genutzt. Die aktiven Komponenten sind von Extreme Networks (Switching) sowie von Sophos für die Anbindung der Außenstandorte und das Routing der verschiedenen Netzwerke.

Die Server sind mit Adapterteaming konfiguriert (2x10GB/s mehrere Teams), die Arbeitsstationen mit 1Gbit/s an das Netzwerk angeschlossen.

WLAN wird über Access Points und einen Wireless-Controller von Extreme Networks bereitgestellt. Die Authentifizierung am Netzwerk (Kabelgebunden und Kabellos) erfolgt mittels 802.1x mit zertifikatsbasierten Authentifizierungsmethoden für die firmeneigenen Geräte.

15. Drucker

In der WFBB sind 16 Netzwerkdrucker installiert. Die Netzwerkdrucker werden über einen zentralen Printserver angesteuert, auf dem ebenfalls ein zentrales Print-System der Firma Triumph-Adler ist. Druckaufträge werden per FollowMe-System auf die jeweiligen Drucker verteilt. Für die Drucktechnik einschließlich der Software gibt es einen gesonderten Wartungsvertrag.

16. Server

Die Server sind auf Hardware der Firma Dell installiert. Zusätzlich wird ein EMC² Storage eingesetzt.

17. Unterbrechungsfreie Stromversorgung

In jedem der beiden Technikräume sind zwei unterbrechungsfreie Stromversorgungen von APC verbaut. Alle Geräte und Komponenten sind mit mindestens einem Netzteil an eine der USVen angeschlossen.

Auf den Hardware-Servern wird die APC Powerchute Software verwendet, um ein kontrolliertes Herunterfahren der Server bei Stromausfällen zu ermöglichen.

18. Arbeitsstationen

In der WFBB sind derzeit 200 geleaste HP-Notebooks, sowie vereinzelte Mini-PCs, Standrechner und Tablets. Als Betriebssystem wird Microsoft Windows 11 Enterprise genutzt und als Standardsoftware Office 2024.

19. Endpoint Protection

Als Endpoint Protection wird die Sophos Endpoint/Server Protection mit Managed Detection and Response von Sophos eingesetzt. Im Zusammenspiel mit den eingesetzten Sophos Firewalls wird die Heartbeat-Technologie der Endpoint Protection verwendet, um benutzerbasierte Firewallregeln konfigurieren zu können.

20. Sonstige Dienste

Server und PCs werden mittels WSUS und WPP auf ein aktuelles Patchlevel in Betriebssystem und diverser Drittanbietersoftware aktualisiert. Weiterhin gibt es ein Netzwerkmanagementsystem zur zentralen Verwaltung der Switching-Infrastruktur.

Für den Austausch von Dateien wird eine Lösung von Zertificon, Z1 SecureHub, in der DMZ bereitgestellt. Des Weiteren existiert derzeit ein proaktives Monitoring auf Basis von PRTG mit dem derzeitigen Dienstleister. Außerdem wird das Dokumentenmanagementsystem Docuware eingesetzt. Das DMS wird durch einen separaten Dienstleister betreut.

21. Verträge

Software:

Adobe-Rahmenvertrag Land Brandenburg

Microsoft Enterprise Agreement

Cisco Duo

Cisco Meraki

Citrix

Sophos Endpoint Protection und MDR

SoftwareOne Select-Rahmenvertrag Land Brandenburg

GEFAK Wartungs- u. Betreuungsvertrag KWIS.net

SMS Reisekosten-Software

DATEV Unterauftrag Steuerberater

Leasing:

Triumph-Adler Druck- und Kopiertechnik

DUBRAU GmbH Leasing Arbeitsplatzcomputer

Internet:

Deutsche Telekom RegionalCenter in Neuruppin

Enviatel GmbH DSL RegionalCenter in Cottbus

Enviatel GmbH DSL RegionalCenter in Spreetal

Telta Citynetz GmbH RegionalCenter in Eberswalde

Deutsche Telekom RegionalCenter in Frankfurt

Deutsche Telekom DSL Friedrich-Engels-Str. Potsdam

Versatel Babelsberger Str. Potsdam

WEB-Hosting

hosteurope

Vertraulich