Level 400 · Expert Security Analysis

SharePoint Subscription Edition Sicherheitsanalyse für die Hausfeld Gruppe GmbH & Co. KG

Definitive technische Referenz für die Härtung, Protokollbewertung, Bedrohungsmodellierung und Überwachung einer SharePoint Subscription Edition Farm auf Azure IaaS nach vollständiger Ablösung des früheren Rechenzentrums in Düsseldorf.

Letzte Aktualisierung: 15.06.2026 **Geschätzte Lesezeit:** ca. 42 Minuten

Zielgruppe: IT Security, SharePoint Administrators, Infrastructure Architects, SOC, IAM

> **Wesentliche Kernaussage**
>
> Für das Zielbild der Hausfeld Gruppe ist `OIDC mit Microsoft Entra ID` die primäre Authentifizierung. Kerberos bleibt nur für interne, streng kontrollierte Server-zu-Server- oder Intranet-Szenarien zulässig. NTLM, Legacy SOAP, unnötiges WebDAV und unsegmentierte East-West-Kommunikation sind in Azure IaaS nicht vertretbar.

1. Einleitung & Zielsetzung

1. Einleitung & Zielsetzung

Diese Analyse bewertet die Sicherheitslage einer SharePoint Subscription Edition (SPSE) Umgebung der fiktiven **Hausfeld Gruppe GmbH & Co. KG** nach einer vollständigen Migration von einem historisch gewachsenen On-Premises-Betrieb in Düsseldorf auf **Azure IaaS Virtual Machines** in der Region West Europe. Fokus ist nicht nur das klassische SharePoint Hardening, sondern die Gesamtrisikolage im Zusammenspiel aus Identity, Netzwerk, Betriebssystem, Farm-Topologie, SQL Always On und Monitoring.

- **Zweck:** Ableitung eines belastbaren Sicherheitszielbilds, Identifikation architektureller Rest-Risiken und Priorisierung konkreter Remediation-Maßnahmen.

- **Scope:** SharePoint Subscription Edition Farm auf Azure IaaS, inklusive Azure Netzwerk, Windows Server, SQL Server Always On, Active Directory, Entra ID Federation/OIDC, ULS, SIEM und betriebliche Sicherheitsprozesse.
- **Nicht im Scope:** SharePoint Online, Microsoft 365 Multi-Tenant Administration, generische Secure Coding Guidelines für Eigenentwicklungen ohne SharePoint-Bezug.
- **Zielgruppe:** CISO-nahe Fachbereiche, IAM/AD Engineers, SharePoint-Farm-Admins, Azure Landing Zone Architekten, SOC/DFIR, SQL DBAs.

> **Hausfeld-spezifischer Kontext**
>
> Die Hausfeld Gruppe betreibt seit 2007 SharePoint für Intranet, Dokumentenmanagement, Vertriebsberater-Portal, Produktdokumentation, HR Self-Service, Projektmanagement und Compliance-Workflows. Mit rund 15.000 Benutzern – inklusive externer Sales Consultants – ist die Plattform nicht bloß Kollaboration, sondern ein geschäftskritischer Produktionsservice.

Der historische Versionspfad `2007 → 2010 → 2013 → 2016 → SPSE` impliziert erfahrungsgemäß Altlasten: vererbte Web Applications, Legacy Alternate Access Mappings, alte Claims Provider, benutzerdefinierte Lösungen, verbliebene `_vti_bin`-Integrationen, veraltete Authentifizierungs-Fallbacks, großzügige Servicekonto-Berechtigungen und nicht mehr benötigte Features. Gerade nach einer Infrastrukturmigration auf Azure dürfen diese Muster nicht "mitgenommen und neu verpackt", sondern müssen aktiv reduziert werden.

2. Ausgangssituation

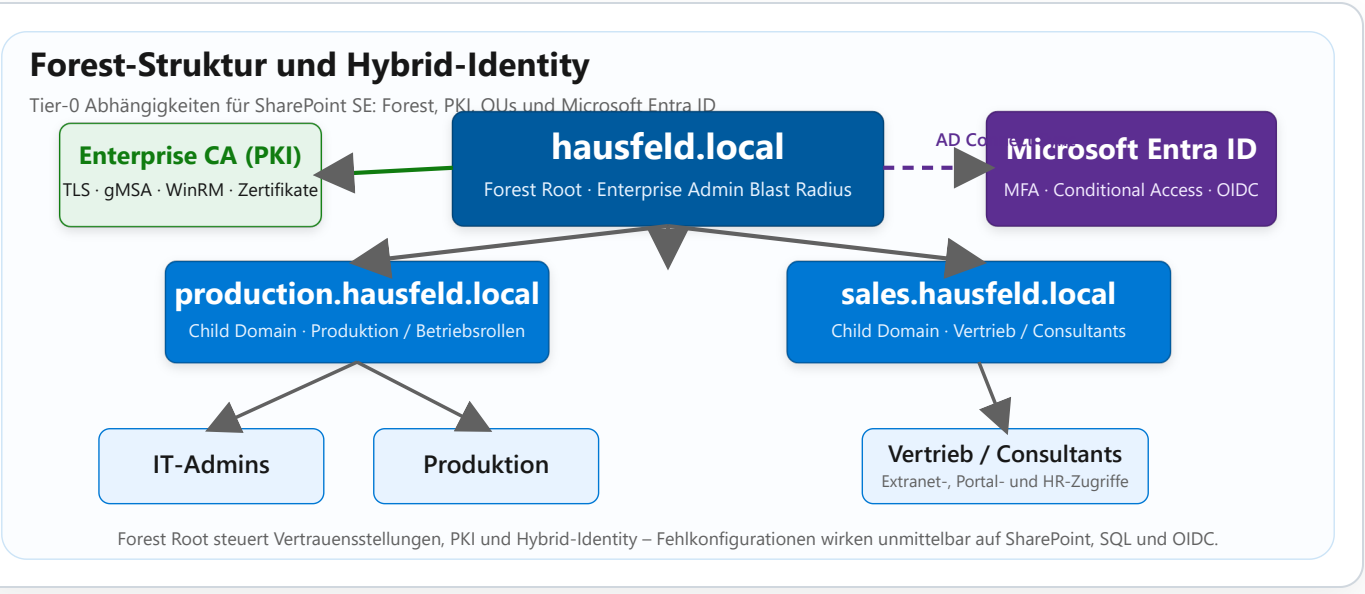
2. Ausgangssituation

Die Hausfeld Gruppe ist ein familiengeführter Premium-Hausgerätehersteller aus Düsseldorf mit rund 8.000 Mitarbeitenden, über 50 Landesgesellschaften und einem stark beratungsgetriebenen Direktvertriebsmodell. Technisch resultiert daraus eine heterogene Identity- und Kollaborationslandschaft, in der interne Mitarbeitende, externe Handelsvertretungen, HR, Legal und Compliance-Workflows auf dieselbe SharePoint-Plattform zugreifen.

2.1 AD-Forest- und Domain-Struktur

Ebene	Ausprägung im Szenario	Sicherheitsrelevanz
Forest	`hausfeld.local`	Enterprise Admin / Schema Admin Exposure muss minimiert werden; Forest ist der eigentliche Blast-Radius.
Child Domains	`production.hausfeld.local`, `sales.hausfeld.local`	Historisch separierte Administrations- und Vertriebsstrukturen; erhöht Komplexität bei SPNs, Gruppenauflösung, Trust Transitivity und AuthN-Troubleshooting.
Identity Source	AD DS in Azure IaaS, Synchronisation ausgewählter Identitäten nach Microsoft Entra ID	Ermöglicht OIDC/MFA/Conditional Access, erhöht jedoch die Kritikalität von Hybrid-Identity-Hardening.
PKI	Interne Enterprise CA für interne TLS-, WinRM-, gMSA- und ggf. Client-Zertifikate	Fehlkonfiguration der PKI wirkt sich unmittelbar auf TLS, Smart Card, JEA, SQL, STS und OIDC-Trusts aus.

Abbildung 1: Active-Directory-Forest, Hybrid-Identity und PKI-Beziehungen

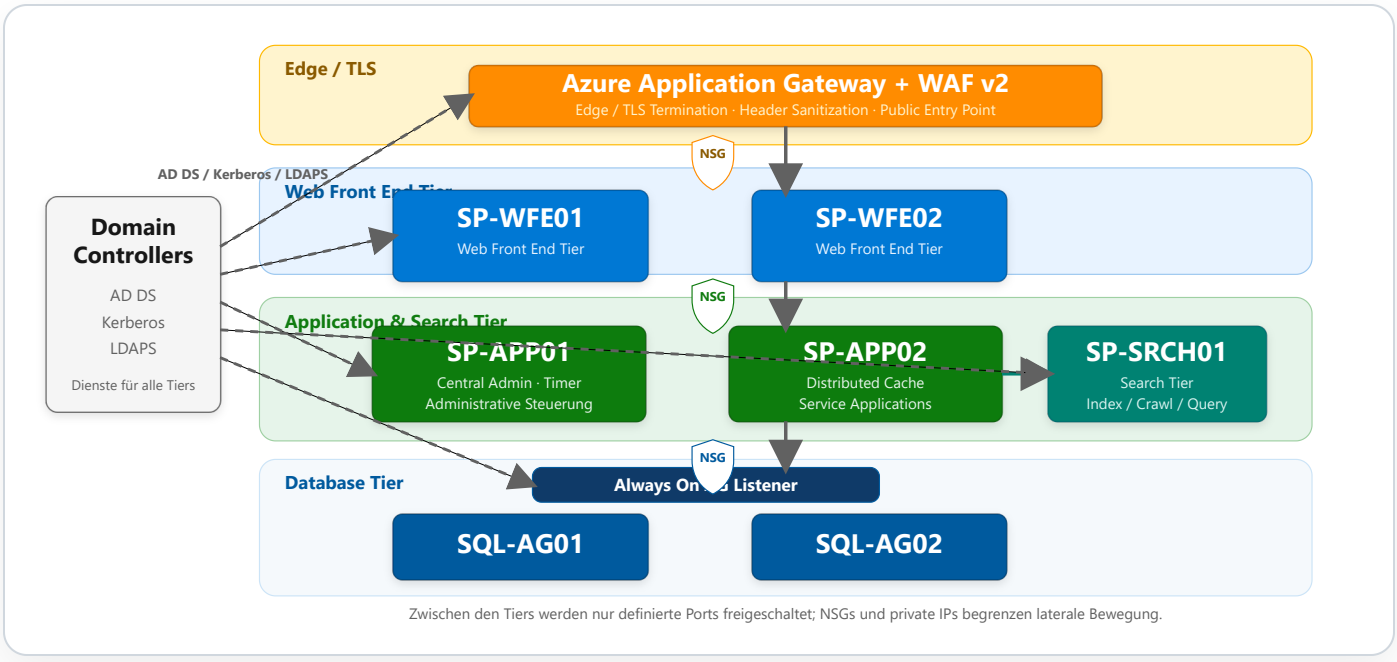


2.2 Ziel-Topologie der SharePoint-Farm in Azure

Tier	Server	MinRole / Funktion	Sicherheitskommentar
Edge / Reverse Proxy	Azure Application	TLS Termination/Bridging, WAF, Listener, Header Sanitization	Öffentlich exponierter Einstiegspunkt; Backends ausschließlich private IPs.

Tier	Server	MinRole / Funktion	Sicherheitskommentar
	Gateway WAF v2		
Web Front End	SP-WFE01, SP-WFE02	Front-end with Distributed Cache offload disabled on WFE	Keine Administrationsarbeiten direkt; Browser Requests, REST, CSOM, SOAP nur via WAF/AppGW.
Application	SP-APP01, SP-APP02	Application + Central Admin + Timer + ggf. Distributed Cache	Höchstes Privilege Aggregation Risk; JEA/JIT obligatorisch.
Search	SP-SRCH01	Dedicated Search	Index enthält hochsensible Metadaten; keine allgemeine Administrationsnutzung.
Database	SQL-AG01, SQL-AG02	SQL Server Always On Availability Group	TDE, TLS, Audit und minimale Surface Area zwingend.

Abbildung 2: Ziel-Topologie der SharePoint-Farm auf Azure IaaS



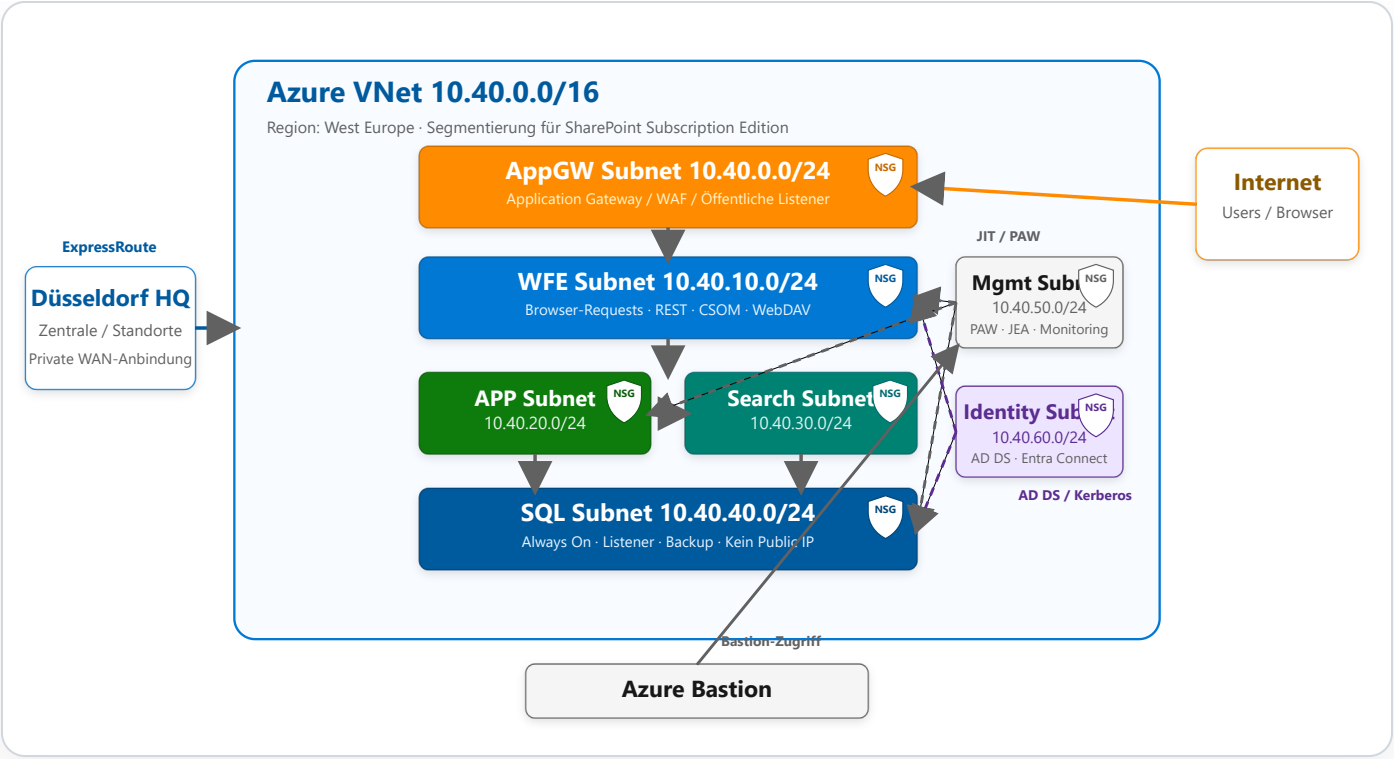
2.3 Netzwerkarchitektur

Ein realistisches Azure VNet für die Hausfeld Gruppe ist beispielsweise `10.40.0.0/16` mit segmentierten Subnetzen:

Subnetz	Beispiel	Zweck	Kontrollen
App Gateway	10.40.0.0/24	Öffentlicher Eintrittspunkt / WAF	Nur 443 inbound aus Internet; Backend nur WFE:443.
WFE	10.40.10.0/24	HTTP Pipeline, REST, CSOM, WebDAV	Kein direkter RDP-Zugriff aus User-Netzen; nur JIT/PAW.
APP	10.40.20.0/24	Service Apps, Timer Jobs, Central Admin	Hochsegmentiert; WinRM nur aus Management-Subnetz.
Search	10.40.30.0/24	Crawl/Query Components	Nur definierte Search-Ports zu WFE/APP/SQL.
SQL	10.40.40.0/24	Always On, Listener, Backup	Kein Public IP; nur SharePoint und DBA-PAWs.
Management	10.40.50.0/24	PAW, Bastion/Jump, Monitoring	Source of truth für RDP/WinRM/JEA.
Identity	10.40.60.0/24	Domain Controller, ADFS/Entra Connect falls vorhanden	Isoliert, höchste Priorität für Tier-0 Kontrollen.

> **Migrationseffekt**
>
> Auch wenn das alte Düsseldorfer Datacenter abgeschaltet wurde, bleibt eine abgesicherte Anbindung an die Düsseldorfer Zentrale und internationale Standorte erforderlich. ExpressRoute ist für planbare, private Konnektivität vorzuziehen; Site-to-Site VPN ist nur Fallback oder für kleinere Landesgesellschaften geeignet. Netzwerkflüsse müssen nach der Migration neu bewertet werden, weil “früher intern” in Azure nicht automatisch “vertrauenswürdig” bedeutet.

Abbildung 3: Segmentierte Azure-VNet-Architektur für SharePoint SE



2.4 Migrationskontext und Sicherheitsimplikationen

- **Content Database Attach / Farm Modernisierung:** Altlasten aus Legacy Web Applications und Solutions können stillschweigend mitgewandert sein.
- **DNS & TLS Cutover:** Zertifikate, AAMs, Host Header Bindings und SPNs müssen vollständig neu validiert werden.
- **Externe Consultants:** Historisch gewachsene Extranet-Konzepte mit FBA/NTLM sind nach Azure-Migration nicht mehr akzeptabel; MFA/Conditional Access ist Pflicht.
- **Operational Shift:** Backups, Patching, Defender, Sentinel, NSG Flow Logs und JIT Access gehören zur Zielarchitektur, auch wenn sie im On-Prem-Betrieb nie benötigt wurden.

3. Zugriffsmethoden und Protokolle im Detail

3. Zugriffsmethoden und Protokolle im Detail

SharePoint bietet funktional nicht nur “Webzugriff”, sondern eine Vielzahl unterschiedlicher Protokoll- und API-Oberflächen. In Sicherheitsbewertungen werden diese häufig als gleichwertig

behandelt; tatsächlich unterscheiden sie sich massiv hinsichtlich Session Handling, Authentisierung, Token-Schutz, Protokollverbosität und Missbrauchspotenzial.

3.1 HTTP/HTTPS Web-Zugriff

- **Technische Funktionsweise:** Browser sprechen SharePoint typischerweise via `HTTPS 443/TCP` an. Authentisierung erfolgt per Negotiate/Kerberos, OIDC Redirect, SAML Redirect oder FBA/Cookie. Nach erfolgreicher Authentisierung werden FedAuth/rtFa/Session Cookies und ggf. Request Digest Tokens für POST-Operationen eingesetzt.
- **Default-Konfiguration:** Historisch existieren oft parallel `HTTP:80` und `HTTPS:443`. SPSE selbst erzwingt TLS nicht automatisch. Cipher Suites richten sich nach Windows Schannel und nicht nach SharePoint.
- **Sicherheitsimplikationen:** Ohne HSTS, TLS 1.2+, moderne Cipher Suites, Cookie Security Flags, Host Header Validation und WAF bleibt die primäre Angriffsfläche offen. Mögliche Schwächen: Downgrade, Session Hijacking, Verb Tampering, verbose error pages, Response Header Leakage.
- **Risikostufe:** Hoch bei fehlendem TLS Hardening; Mittel im gehärteten Zielbild.

TLS HARDENING – REGISTRY

```
; Nur TLS 1.2+ erlauben
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.0\Server\Enabled = 0
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.1\Server\Enabled = 0
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.2\Server\Enabled = 1
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.2\Client\Enabled = 1

; HSTS am Reverse Proxy / App Gateway Header Rewrite
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

3.2 WebDAV

- **Technik:** SharePoint exponiert Dokumentbibliotheken über WebDAV-Methoden wie `PROPFIND`, `OPTIONS`, `LOCK`, `UNLOCK`, `PUT` und Namespace-Erweiterungen unter HTTP(S). Windows Explorer kann Bibliotheken als Netzlaufwerk oder Web Folder darstellen.

- **Default:** Nicht jede Farm nutzt WebDAV aktiv, aber Bibliotheken sind häufig implizit kompatibel. In vielen Altumgebungen ist der Zugriff aus Gewohnheit erlaubt, obwohl moderne OneDrive-Sync- oder Browser-Workflows genügen würden.
- **Sicherheitsimplikationen:** WebDAV erleichtert Bulk Exfiltration, ist ein klassisches Ziel für NTLM Relay, umgeht teilweise browserseitige Sicherheitskontrollen, schafft Dateisystem-ähnliche Benutzererwartung und kann von unsicheren Client-Systemen missbraucht werden.
- **Risikostufe:** Hoch , wenn aus unkontrollierten Netzen erreichbar oder für externe Consultants offen.

3.3 CSOM (Client-Side Object Model)

- **Technik:** .NET CSOM nutzt Assemblies wie `Microsoft.SharePoint.Client.dll` ; JavaScript CSOM nutzt Browser-seitige Client-APIs. CSOM serialisiert Anfragen als XML/JSON-Batches an `/_vti_bin/client.svc/ProcessQuery` .
- **Authentisierung:** AuthN folgt dem Web-Kontext (Kerberos/OIDC/SAML/FBA). Tokens/Cookies werden vom Client gehalten; bei App-Only-Szenarien kann OAuth/OIDC indirekt beteiligt sein. Im Browser ist CSOM an Session Cookies gebunden, im Skriptkontext oft an gespeicherte Credentials oder Token Acquisition Flows.
- **Security Notes:** CSOM ist extrem mächtig für Enumeration, Permission Mining, Bulk Download und Metadaten-Manipulation. Rate Limits klassischer Art existieren on-prem nicht in gleichem Maße wie in M365.
- **Risikostufe:** Hoch aus Sicht Datenzugriff und Automatisierungsmissbrauch.

3.4 REST API (`/_api/`)

- **Technik:** SharePoint REST basiert auf OData-Endpunkten wie `/_api/web/lists` , `/_api/search/query` oder `/_api/web/GetFolderByServerRelativeUrl(...)` . Schreibende Operationen erfordern typischerweise ein `X-RequestDigest` -Token, das über `/_api/contextinfo` bezogen wird.
- **Default:** Endpunkte sind aktiv, sobald die Web Application erreichbar ist. Sie erfordern nicht automatisch separate Härtung.
- **AuthN/Token Handling:** Browser nutzen FedAuth/rtFa-Cookies; moderne Integrationen sollten OAuth Bearer Tokens bzw. OIDC-basierte Tokenflüsse verwenden. Ohne explizite Beschränkung können Skripte sehr große Datenmengen seriell oder parallel abziehen.
- **Risikostufe:** Hoch für Exfiltration und Permission Enumeration; Mittel im Zielbild mit OAuth, WAF, Logging und Anomalieerkennung.

REST – DIGEST UND BEARER TOKEN

```
# Beispiel: POST mit Request Digest in einer internen Session
Invoke-RestMethod -Uri "https://intranet.hausfeld.com/_api/contextinfo" `
  -Method Post -Headers @{Accept="application/json;odata=verbose"}

# Zielbild: Bearer Token über OIDC/OAuth
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIs...
```

3.5 SOAP/ASMX Web Services

- **Technik:** Legacy Services unter `/_vti_bin/*.asmx` wie `Lists.asmx`, `Copy.asmx`, `Webs.asmx` oder `UserGroup.asmx` stellen ältere SOAP-Schnittstellen bereit.
- **Default:** In legacy-lastigen Farmen häufig weiter erreichbar, obwohl kaum noch legitime Abhängigkeiten bestehen.
- **Warum gefährlich:** Alte Integrationen erzwingen oft NTLM/Basic-ähnliche Bedienmuster, liefern überverbose Fehlermeldungen, erlauben systematische Enumeration und verlängern die Lebensdauer unsicherer Client-Software. Für Angreifer sind ASMX-Endpunkte lohnende Recon- und Data Access-Ziele.
- **Risikostufe:** `Hoch` ; wenn keine nachweisbare Abhängigkeit existiert, sollten diese Endpunkte nicht veröffentlicht werden.

3.6 PowerShell & PnP

- **Technik:** SharePoint Management Shell arbeitet lokal auf Farm-Servern mit hoher Berechtigung. PnP PowerShell nutzt CSOM/REST/OAuth und eignet sich für Remote Automation, Content Operations und Tenant-/Site-Administration.
- **Default:** Farm-Administratoren erhalten schnell breiten Shell-Zugriff; historisch werden Servicekonten und lokale Administratorrechte oft vermischt.
- **Sicherheitsimplikationen:** Missbrauch von `Add-SPShellAdmin`, unsignierte Skripte, interaktive Nutzung von Service Accounts und WinRM ohne JEA führen unmittelbar zu Privilege Escalation und lateraler Bewegung.
- **Risikostufe:** `Kritisch` für Betriebskonten und Administrative Paths.

3.7 RPC over HTTP / Outlook Integration

- **Technik:** Historische Outlook/SharePoint-Integration umfasste Alerts, Kalenderüberlagerung, Kontaktlisten und List Synchronization. Praktisch laufen moderne Clients meist über HTTPS-basierte Web Services, EWS/Graph-artige Flows oder lokale Protokollhandler.

- **Default:** Alte Integrationspfade bleiben oft aktiviert, obwohl funktional kaum genutzt.
- **Sicherheitsimplikationen:** RPC-/MAPI-nahe Altpfade sind schwer zu überwachen, schlecht dokumentiert und neigen zu impliziten NTLM-Fallbacks. Jede Legacy Outlook-Integration sollte explizit inventarisiert werden.
- **Risikostufe:** Mittel bis Hoch je nach Legacy-Abhängigkeit.

3.8 Search Protocol (OpenSearch/RSS)

- **Technik:** SharePoint Search bietet Query- und Crawl-Schnittstellen, Ergebnisfeeds, RSS/OpenSearch-ähnliche Consumption Patterns sowie serverseitige Indizierung. Der Suchindex speichert Metadaten und Security Trimming-Informationen.
- **Default:** Search ist meist global aktiviert; Feeds und Query-Parameter werden selten restriktiv überprüft.
- **Sicherheitsimplikationen:** Search ist ein Force Multiplier für Recon. Falsch konfigurierte Security Trimming-Einstellungen, Crawl Rules, Query Suggestions oder Result Sources können Information Disclosure begünstigen. Selbst wenn Dokumente nicht direkt ladbar sind, können Titel, Authors, Pfade und Snippets wertvolle Daten liefern.
- **Risikostufe:** Hoch für Informationsabfluss.

3.9 SMTP Integration

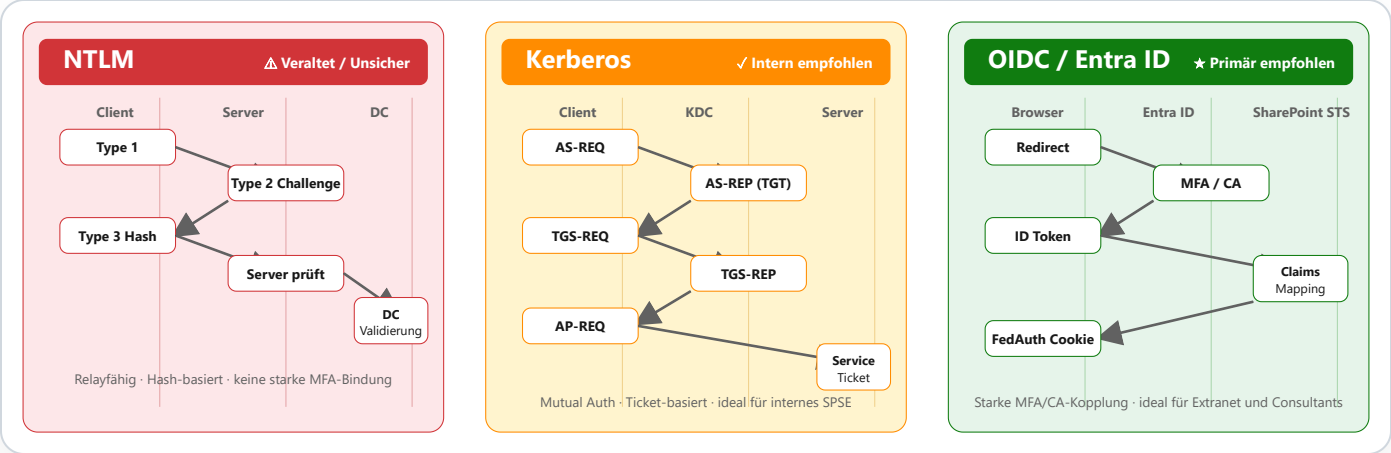
- **Technik:** SharePoint unterstützt ausgehende E-Mails (Alerts, Workflows, Einladungen) und eingehende E-Mails für Listen/Bibliotheken als Mail Targets. Technisch relevant sind SMTP Relays, Drop Directories, MX-Routing und Attachment Handling.
- **Default:** Outgoing Mail ist häufig aktiv; Incoming Mail wird in DMS-/Scan-Szenarien oft vergessen, bleibt aber konfiguriert.
- **Sicherheitsimplikationen:** Missbrauchbare SMTP Relays, gefälschte Absender, ungescannte Anhänge, indirekte Malware-Zustellung oder Workflow-Triggering über E-Mail sind reale Risiken. In Azure ist ein offenes SMTP-Design zusätzlich reputationskritisch.
- **Risikostufe:** Mittel bis Hoch je nach Relay-Modell und E-Mail-Inbound-Nutzung.

4. Authentifizierungsprotokolle ▾

4. Authentifizierungsprotokolle

Für SPSE auf Azure IaaS ist die Wahl des Authentifizierungsprotokolls die zentrale Sicherheitsentscheidung. Sie beeinflusst nicht nur den Login, sondern auch Delegation, Service-to-Service-Kommunikation, API-Nutzung, Monitoring, MFA-Durchsetzung und die Angriffsfläche für Credential Theft.

Abbildung 4: Vergleich von NTLM, Kerberos und OIDC / Entra ID



4.1 NTLM

Paketfluss: `Type 1 (Negotiate)` → `Type 2 (Challenge)` → `Type 3 (Authenticate)`. Der Client beweist Besitz des Passwort-Hashes, ohne das Passwort im Klartext zu senden. NTLMv2 verbessert Challenge-Response und Session Security gegenüber NTLMv1, bleibt aber hashbasiert und relayfähig.

- **Default-Fallback:** In IIS/Windows ist `Negotiate` häufig aktiviert; schlägt Kerberos fehl, fällt der Stack auf NTLM zurück. Genau dieses “silent fallback” hält NTLM künstlich am Leben.
- **Schwachstellen:** Pass-the-Hash, NTLM Relay, fehlende gegenseitige Authentisierung, schwache Bindung an Channel/TLS, schlechte MFA-Kompatibilität.
- **NTLMv1 vs NTLMv2:** NTLMv1 ist kryptographisch unzureichend und muss vollständig deaktiviert sein. NTLMv2 ist nur “weniger schlecht”, nicht zukunftssicher.
- **Detektion:** Windows Event IDs `4624` mit `AuthenticationPackageName=NTLM`, `4776` auf Domain Controllern, IIS/W3C Logs mit Negotiate/NTLM Mustern, Sentinel-Korrelation.

NTLM ERKENNEN UND DEAKTIVIEREN

```
# Erkennung: DC / Server
Get-WinEvent -LogName Security | Where-Object { $_.Id -in 4624,4776 }

# Härtung: Senden von NTLM blockieren
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0\RestrictSendingNTLMTraffic = 2
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\LmCompatibilityLevel = 5
```

```
# Audit-only vor vollständiger Abschaltung
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0\AuditReceivingNTLMTraffic = 2
```

> **Bewertung**
>
> In einer neu auf Azure IaaS migrierten Farm ohne legitime Legacy-Zwänge ist aktives NTLM ein Kritisch-Risiko. Es ermöglicht moderne Relay- und Lateral-Movement-Angriffe trotz "Cloud-Migration".

4.2 Kerberos

Paketfluss: `AS-REQ` → `AS-REP` (TGT) → `TGS-REQ` → `TGS-REP` (Service Ticket) → `AP-REQ` → `AP-REP` optional. Kerberos bietet Mutual Authentication, Delegationsmodelle und reduziert Passwort-Exposure im Vergleich zu NTLM.

- **SPN-Konfiguration:** Für Web Applications typischerweise `HTTP/intranet.hausfeld.com` auf das Application Pool Identity / gMSA. Falsch gesetzte oder doppelte SPNs führen zu Kerberos-Fails und NTLM-Fallback.
- **Delegation:** Unconstrained Delegation ist zu vermeiden. Präferiert: Constrained Delegation oder besser Resource-Based Constrained Delegation (RBCD), wenn wirklich erforderlich.
- **Angriffe:** Kerberoasting (TGS-REP offline crackbar bei schwachen Service Account Passwörtern), Golden Tickets (krbtgt kompromittiert), Silver Tickets (Service Key kompromittiert), Pass-the-Ticket, AS-REP Roasting bei Accounts ohne Preauth.
- **Detektion:** Events `4768`, `4769`, `4771`, ungewöhnliche Ticket Encryption Types, TGS-Spikes für SPNs der SharePoint/SQL-Dienste.

SPN- UND DELEGATIONSBEISPIELE

```
setspn -S HTTP/intranet.hausfeld.com HAUSFELD\sp-web$
setspn -S HTTP\sp-wfe01.hausfeld.local HAUSFELD\sp-web$
setspn -S MSSQLSvc/sql-ag-listener.hausfeld.local:1433 HAUSFELD\sqlsvc$

# Unconstrained Delegation verbieten, gMSA bevorzugen
Get-ADComputer SP-WFE01 -Properties
TrustedForDelegation,PrincipalsAllowedToDelegateToAccount
Get-ADServiceAccount sp-web -Properties ServicePrincipalNames
```

4.3 Claims-Based Authentication (SAML 2.0)

- **Technik:** Browser wird an einen Identity Provider (IdP) umgeleitet, erhält ein signiertes SAML Assertion Token und präsentiert es dem SharePoint Security Token Service (STS) bzw. der Vertrauensstellung. Claims Mapping übersetzt Attribute wie UPN, E-Mail, Rollen oder SID in SharePoint Claims.
- **Sicherheitsmerkmale:** Signierte Assertions, zentrale AuthN-Policy, potenziell MFA-fähig. Schwächen entstehen bei Replay-fähigen Tokens, zu langen Token-Lifetimes, unsauberem Audience Restriction Design und ungenügender Zertifikatspflege.
- **Risiken:** Token Replay, Zertifikatsablauf, Claim Inflation, Legacy Libraries/Apps ohne SAML-Kompatibilität, komplexe Fehlersuche.

4.4 OIDC mit Microsoft Entra ID (empfohlen)

Empfohlenes Primärmodell. OIDC ermöglicht moderne Browser- und API-nahe Authentisierung mit Entra ID, MFA, Conditional Access, Sign-in Risk Policies und sauberem Claim-Mapping. Für externe Sales Consultants ist dies die strategisch richtige Variante, weil sie Identity Governance, Access Reviews und starken Session-Schutz nativ unterstützt.

- **Flow:** Browser → App Gateway/WFE → Redirect zu Entra ID → Benutzer authentisiert sich (inkl. MFA/Conditional Access) → ID Token/Authorization Code → SharePoint Trusted Identity Token Issuer → lokale Claims-Transformation → FedAuth Session.
- **Konfigurationspunkte:** App Registration, Redirect URI, Zertifikat/Signing Material, Claims Mapping, Identifier Claim, Reply URL, Token Lifetime, Group Claims Design, Guest/Consultant Governance.
- **Sicherheitsvorteile:** Phishing-resistentere Faktoren, zentrale Governance, Device-/Risk-basierte Policies, bessere Telemetrie in Entra Sign-in Logs und Sentinel.
- **Risiken:** Falsches Claims Mapping, übergroße Token, fehlerhafte App Registration Berechtigungen, unkontrollierte Guest-Zugriffe, unzureichende Zertifikatsrotation.

POWERSHELL – OIDC PROVIDER IN SPSE

```
# OIDC Authentication Provider for SharePoint SE
$cert = New-SelfSignedCertificate -Subject "CN=SharePointOIDC" `
  -CertStoreLocation "Cert:\LocalMachine\My" -KeyExportPolicy Exportable `
  -KeySpec Signature -KeyLength 2048 -KeyAlgorithm RSA -HashAlgorithm SHA256

$oidcProvider = New-SPTrustedIdentityTokenIssuer -Name "EntraID-OIDC" `
  -Description "Microsoft Entra ID OIDC" -ImportTrustCertificate $cert `
  -ClaimsMappings $emailClaimMap, $upnClaimMap, $sidClaimMap, $roleClaimMap `
  -IdentifierClaim $emailClaimMap.InputClaimType `
```

```
  -DefaultClientIdentifier $clientId `
  -RegisteredIssuerName $oidcMetadataEndpoint
```

POWERSHELL – CLAIM MAPPING BEISPIEL

```
$emailClaimMap = New-SPClaimTypeMapping `
  -IncomingClaimType
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" `
  -IncomingClaimTypeDisplayName "E-Mail" -SameAsIncoming

$upnClaimMap = New-SPClaimTypeMapping `
  -IncomingClaimType "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn" `
  -IncomingClaimTypeDisplayName "UPN" -SameAsIncoming
```

4.5 Forms-Based Authentication (FBA)

- **Technik:** ASP.NET Membership-/Role-Provider, Login-Formular, Auth Cookie. Historisch genutzt für Extranet-Szenarien.
- **Risiken:** Passwortspeicher, Brute Force, Credential Stuffing, schwache Session Cookies, Custom Provider Schwachstellen, mangelnde MFA-Integration.
- **Bewertung:** Für die Hausfeld Gruppe nur als Legacy-Ausnahme tolerierbar; strategisch ablösen.

4.6 Certificate-Based Authentication

- **Technik:** Client-Zertifikate oder Smart Cards binden Authentisierung an eine PKI und häufig an Hardware (TPM/Smart Card). SharePoint selbst nutzt dies typischerweise über vorgelagerte Komponenten oder AD-integrierte Zertifikatsanmeldung.
- **Sicherheitsvorteile:** Starke kryptographische Bindung, gute Resistenz gegen Passwortdiebstahl, geeignet für Admin-PAWs.
- **Herausforderungen:** PKI-Lifecycle, CRL/OCSP Verfügbarkeit, Zertifikat-Mapping, externer Benutzerkreis, Browser-Kompatibilität.

5. Ports und Netzwerkprotokolle (Complete Reference)

5. Ports und Netzwerkprotokolle (Complete Reference)

Die folgende Referenz ist für die Hausfeld-Farm als Baseline für NSGs, Windows Firewall, Azure Firewall, NVA-Regeln und Flow-Log-Analysen zu verwenden.

Service	Port	Protocol	Direction	Security Notes
HTTP	80	TCP	Inbound	Nur für Redirect auf HTTPS; niemals Inhaltstransport.
HTTPS	443	TCP	Inbound	TLS 1.2+ erforderlich; HSTS; WAF davor.
SQL Server	1433	TCP	Internal	AG Listener nur intern; TLS erzwingen.
SQL Browser	1434	UDP	Internal	Wenn möglich deaktivieren; nur bei Named Instances/Legacy Discovery nötig.
LDAP	389	TCP/UDP	Outbound	Nur temporär für Troubleshooting; produktiv LDAPS bevorzugen.
LDAPS	636	TCP	Outbound	Standard für sichere AD-Kommunikation.
Global Catalog	3268/3269	TCP	Outbound	3269 bevorzugt; für Forest-weite Queries relevant.
Kerberos	88	TCP/UDP	Outbound	Zeit-Synchronität und DNS kritisch.
DNS	53	TCP/UDP	Outbound	Nur interne Resolver; DNS Logging aktivieren.
SMB	445	TCP	Internal	Restriktiv; SMBv1 deaktiviert, Signing/Encryption wo möglich.
RPC	135	TCP	Internal	DCOM nur bei belegbarem Bedarf; Minimierung Pflicht.
RPC Dynamic	49152-65535	TCP	Internal	Range einschränken und hart segmentieren.

Service	Port	Protocol	Direction	Security Notes
Distributed Cache	22233-22236	TCP	Internal	AppFabric/Cache nur zwischen definierten Farm-Knoten.
Search Crawl	56737-56738	TCP	Internal	Niemals exponieren; nur Search-Komponenten.
Search Admin	56737-56741	TCP	Internal	Nur Search ↔ Farm-Kommunikation.
Central Admin	32843-32844	TCP	Internal	Ausschließlich Management-Subnetz/PAW/JIT.
SMTP	25/587	TCP	Outbound	Relay restriktiv; Auth/TLS falls möglich.
NTP	123	UDP	Outbound	Kerberos-relevant; Zeitquelle vertrauenswürdig halten.
WinRM	5985/5986	TCP	Internal	5986 bevorzugt; JEA + Client-Zertifikate/PAW.

> **Architekturregel**
> Jeder dieser Ports muss *gleichzeitig* in NSG, Windows Firewall, ggf. Azure Firewall und Betriebsdokumentation konsistent abgebildet sein. Häufige Schwäche nach Migration: NSG ist restriktiv, Windows Firewall permissiv – oder umgekehrt.

6. Risikobewertung

6. Risikobewertung

Methodisch wird ein klassisches **Likelihood × Impact**-Modell genutzt. Skala 1–5: `1 = niedrig`, `5 = sehr hoch`. Kritisch sind Werte ≥ 16 oder Szenarien mit direktem Domain-/Farm-Admin-Impact.

Wahrscheinlichk \ Auswirkung	1 – Niedrig	2 – Begrenzt	3 – Relevant	4 – Hoch	5 – Sehr hoch
1 – Selten		R8			
2 – Unwahrscheinlic		R7			
3 – Möglich			R6	R4	R3
4 – Wahrscheinlich				R5	R1, R2
5 – Nahezu sicher					

Niedrig Mittel Hoch Kritisch

ID	Feststellung	Likelihood	Impact	Score	Kategorie	Kommentar
R1	NTLM auf WFE/APP/SQL weiterhin aktiv	4	5	20	Kritisch	Ermöglicht Relay, Pass-the-Hash, unsichtbaren Kerberos-Fallback.
R2	Keine harte Netzwerksegmentierung zwischen WFE, APP, SQL	4	5	20	Kritisch	Beschleunigt laterale Bewegung und Privilege Escalation.
R3	SQL-Verbindungen oder Datenbanken unverschlüsselt	3	5	15	Kritisch	Gefährdet Farm-Konfiguration, Secrets, Content und Suchindex.
R4	WebDAV extern exponiert	3	4	12	Hoch	Exfiltration und NTLM Relay werden erheblich erleichtert.

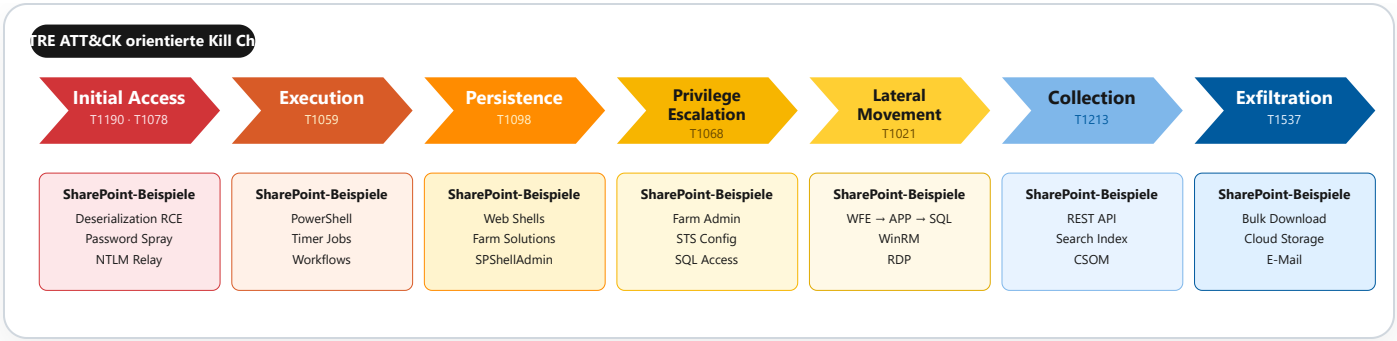
ID	Feststellung	Likelihood	Impact	Score	Kategorie	Kommentar
R5	Patching-Lücken auf Windows/SPSE/SQL	4	4	16	Kritisch	Besonders relevant wegen bekannter Deserialization/RCE-CVEs.
R6	Kein MFA/Conditional Access für Consultants	3	3	9	Mittel	Password Spraying/Credential Stuffing werden wahrscheinlicher.
R7	HSTS fehlt	2	2	4	Niedrig	Kein Primärbruch, aber unnötige Downgrade-/Session-Risiken.
R8	Verbose Error Pages / Standard-Logging	1	2	2	Niedrig	Unterstützt Recon und erschwert Forensik.

7. Angriffsvektoren und Bedrohungsszenarien

7. Angriffsvektoren und Bedrohungsszenarien

Die nachfolgenden Szenarien sind spezifisch für eine SPSE-Farm auf Azure IaaS mit historischer AD-Bindung. Jedes Szenario kombiniert technische Ausnutzung mit realistischer Angreifer-Ökonomie. Relevante MITRE ATT&CK Referenzen sind beigefügt.

Abbildung 5: SharePoint-spezifische Angriffskette nach MITRE ATT&CK



7.1 Credential-basierte Angriffe

Pass-the-Hash, **Pass-the-Ticket**, **Credential Stuffing** und **Password Spraying** sind im Hausfeld-Szenario besonders relevant, weil externe Consultants, historische Servicekonten und möglicherweise nicht vereinheitlichte Passwort-Policies zusammentreffen. Angreifer beginnen häufig mit OWA/VPN/Portal-Anmeldeflächen, pivoten dann zu SharePoint und nutzen erfolgreiche Logons für API-basierte Datenentnahme. **MITRE:** T1078, T1110, T1550.

7.2 NTLM Relay Angriffe

Tools wie `ntlmrelayx` leiten eingehende NTLM-Authentisierungen auf SharePoint oder SQL weiter. WebDAV ist ein attraktives Relay-Ziel, weil Clients Dateisystem-ähnliche Verbindungen aufbauen und NTLM-Fallbacks häufig stillschweigend akzeptieren. Mit erfolgreichem Relay lassen sich Rechte prüfen, Inhalte schreiben/lesen oder weitere Protokolle adressieren. **MITRE:** T1557.001, T1021.

7.3 Kerberoasting & AS-REP Roasting

SharePoint-, SQL- und Crawl-Servicekonten mit schwachen oder statischen Passwörtern sind klassische Roast-Ziele. Angreifer fordern TGS-Tickets für SPNs wie `HTTP/intranet.hausfeld.com` oder `MSSQLSvc/sql-ag-listener` an, extrahieren das Ticketmaterial und cracken offline. Accounts ohne Kerberos Pre-Authentication sind zusätzlich AS-REP-Roast-gefährdet. **MITRE:** T1558.003, T1558.004.

7.4 Laterale Bewegung

Ein kompromittierter WFE ist selten das Endziel. Entscheidend ist der Schritt von WFE → APP → SQL bzw. WFE → AD, häufig über lokale Admin-Rechte, ungesicherte WinRM-Endpunkte, gespeicherte Credentials, GPO-Skripte, Scheduled Tasks oder missbrauchbare Farmkonten. In Azure beschleunigen fehlende NSGs, zu breite ASGs und gemeinsame Management-Subnetze die Bewegung. **MITRE:** T1021, T1072, T1080.

7.5 Privilege Escalation

Missbrauchbare SharePoint Designer Workflows, überprivilegierte Site Collection Admins, `Add-SPShellAdmin`, unsichere Custom Solutions, Elevated Privileges in Timer Jobs oder STS-/Farm-Admin-Rechte können Angreifern sehr schnell von Inhaltsrechten zu Farm- oder sogar SQL-/AD-nahen Rechten verhelfen. **MITRE:** T1068, T1548.

7.6 Datenexfiltration

REST API, CSOM und Search sind prädestiniert für Bulk Enumeration und Download. Ein Angreifer muss nicht zwangsläufig Inhalte "brechen"; häufig genügen legitime, aber missbrauchte Berechtigungen. Typisch: `/_api/web/GetFolderByServerRelativeUrl(...)/Files`, Search Queries über sensible Keywords oder massenhafte `FileDownloaded`-Events außerhalb üblicher Arbeitszeiten. **MITRE:** T1537, T1005, T1213.

7.7 Deserialization Attacks

Frühere Schwachstellen wie **CVE-2019-0604** und **CVE-2020-1147** zeigten, dass SharePoint- und .NET-Deserialisierungspfade Remote Code Execution ermöglichen können. Auch wenn die konkreten Lücken gepatcht sind, bleibt das Muster relevant: ungepatchte WFEs + öffentliche Erreichbarkeit + fehlender WAF = unmittelbare Kompromittierungsgefahr. **MITRE:** T1190.

7.8 Server-Side Request Forgery (SSRF)

SSRF kann über Workflow-Komponenten, BCS, Remote Event Receivers, Proxy-konfigurierbare Integrationen oder unsichere Custom Solutions auftreten. In Azure ist dies besonders kritisch, weil ein SSRF-Pfad gegen `169.254.169.254` (Instance Metadata Service, IMDS) gerichtet werden kann. So kann ein Angreifer Managed Identity Tokens oder Infrastruktur-Metadaten missbrauchen. **MITRE:** T1190, T1552, T1528.

7.9 Cross-Site Scripting (XSS)

Persistente XSS über Wiki-Seiten, Content Editor, Script Editor, unsichere Calculated Columns, schlecht validierte Rich-Text-Felder oder Custom Web Parts kann Session Diebstahl, DOM-basierte API-Aufrufe und Admin-Hijacking ermöglichen. In On-Prem-SharePoint sind XSS-Abwehrmechanismen stark von Governance und Customization-Disziplin abhängig. **MITRE:** T1059.007, T1189.

7.10 Azure-spezifische Angriffe

Fehlkonfigurierte NSGs, Public IPs auf Farm-VMs, überprivilegierte Managed Identities, schwache Defender for Cloud Policies oder offene WinRM/RDP-Pfade schaffen Cloud-spezifische Eintrittspunkte. Besonders kritisch ist IMDS Abuse: Kann ein kompromittierter Server Metadaten lesen, sind Tokens und Subscription-seitige Berechtigungen in Reichweite. **MITRE:** T1528, T1552, T1078, T1021.

> **Praxisrelevanz für Hausfeld**
> Das Vertriebsberater-Portal und HR Self-Service kombinieren externen Zugriff, personenbezogene Daten und geschäftskritische Dokumente. Gerade diese Kombination macht Bulk-Download, Token-Missbrauch, Conditional-Access-Umgehung und Suchindex-Recon zu realistischen Szenarien – nicht nur theoretischen.

8. Optimale Protokolle und Methoden

8. Optimale Protokolle und Methoden

Domäne	Empfehlung	Begründung
Primäre Benutzer-Authentifizierung	**OIDC mit Microsoft Entra ID**	MFA, Conditional Access, Sign-In Risk, Governance für externe Consultants.
Sekundäre interne Authentifizierung	**Kerberos** nur intern	Mutual Authentication, kein Hash-Relay wie NTLM; saubere SPN- und Delegationssteuerung.
Legacy Fallback	**NTLM vollständig abschalten**	Reduziert Relay-, PtH- und Fallback-Angriffsfläche.
Transport Security	**TLS 1.2+**, starke Cipher Suites, HSTS	Schützt Cookies, Tokens, REST/CSOM und Admin-Pfade.
API Nutzung	REST mit OAuth/OIDC Bearer Tokens	Bessere Nachvollziehbarkeit und modernes Token Handling.

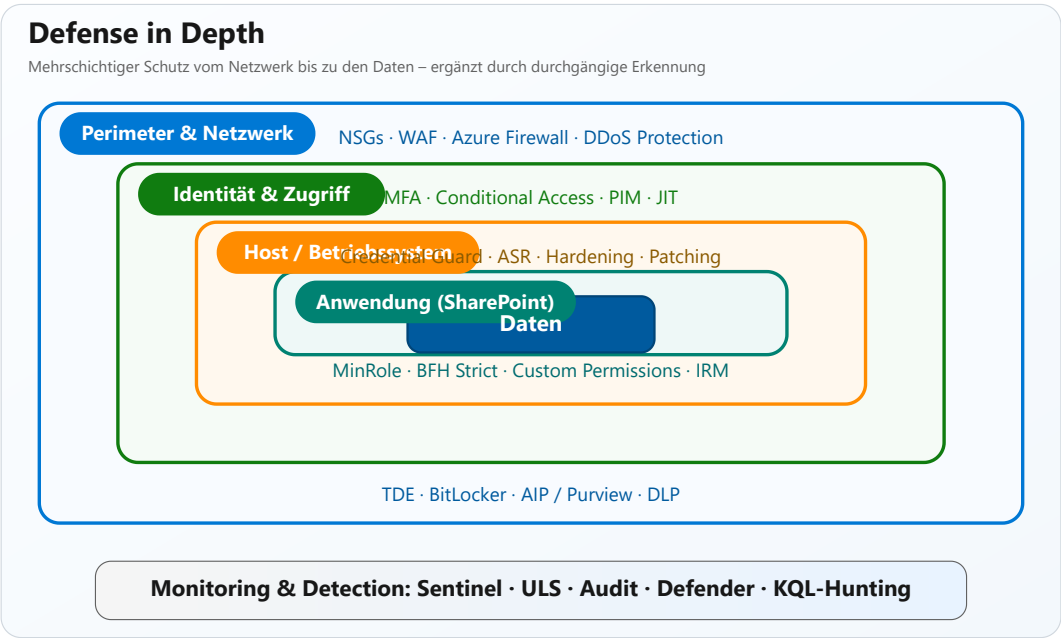
Domäne	Empfehlung	Begründung
Legacy Schnittstellen	SOAP, unnötiges WebDAV, unsichere Outlook-Altpfade deaktivieren	Reduziert Recon- und Missbrauchsoberfläche.
Administrative Automatisierung	PowerShell mit **Constrained Language Mode** und **JEA**	Kontrolliert Befehlsumfang, reduziert Missbrauch von Remote Shells.

> **Empfohlener Migrationspfad für NTLM-Abschaltung**
> 1) Auditieren, 2) SPN-/Kerberos-Fixes durchführen, 3) Pilot-Web-Application auf OIDC umstellen, 4) Externe Nutzer in Entra ID mit MFA überführen, 5) NTLM zunächst auditieren, dann blockieren, 6) WebDAV und ASMX gezielt entkoppeln.

9. Sicherheitsmaßnahmen und Härtung (Comprehensive)

9. Sicherheitsmaßnahmen und Härtung (Comprehensive)

Abbildung 6: Defense in Depth für SharePoint SE auf Azure



9.1 Netzwerkebene

Azure NSG-Regeln

Priority	Source	Destination	Port	Action	Kommentar
100	VPN/ExpressRoute Subnets	SharePoint WFE Subnet	443/TCP	Allow	Nutzerverkehr nur via App Gateway / WAF.
200	SharePoint App Subnet	SQL Subnet	1433/TCP	Allow	Nur AG Listener / SQL Nodes.
300	SharePoint Subnets	DC Subnet	636/TCP	Allow	LDAPS.
400	SharePoint Subnets	DC Subnet	88/TCP,UDP	Allow	Kerberos.
500	Management Subnet	APP/WFE/Search/SQL	5986/TCP	Allow	WinRM nur von PAWs.
600	Management Subnet	APP/WFE/Search/SQL	3389/TCP	Allow	Nur JIT-basiert und zeitlich begrenzt.
4096	*	*	*	Deny	Default Deny als Abschlussregel.

AZ POWERSHELL – NSG REGEL BEISPIEL

```
$nsg = Get-AzNetworkSecurityGroup -Name "nsg-sp-wfe" -ResourceGroupName "rg-
hausfeld-spse"
Add-AzNetworkSecurityRuleConfig -Name "Allow-AppGW-HTTPS" -NetworkSecurityGroup $nsg
`
  -Priority 100 -Direction Inbound -Access Allow -Protocol Tcp `
  -SourceAddressPrefix "10.40.0.0/24" -SourcePortRange "*" `
  -DestinationAddressPrefix "10.40.10.0/24" -DestinationPortRange "443"
$nsg | Set-AzNetworkSecurityGroup
```

- **ASGs:** Verwenden Sie ASGs wie `asg-sp-wfe`, `asg-sp-app`, `asg-sp-search`, `asg-sql`, um Regeln tierbasiert statt IP-basiert zu definieren.
- **Azure Firewall / NVA:** Für Egress Filtering, TLS Inspection (nur selektiv), Threat Intelligence Blocking und zentrale DNAT/SNAT-Kontrolle.
- **WAF via Application Gateway:** Prevention Mode, OWASP CRS 3.2+, Bot Protection, Custom Rules für `/_vti_bin`, Upload-Limits, Header Normalization, End-to-End TLS Bridging.
- **SQL Private Exposure:** Bei SQL auf Azure IaaS kein Public Endpoint. Interne Erreichbarkeit nur über Internal Load Balancer/AG Listener. Für angrenzende PaaS-Dienste (Storage, Key Vault, Backup Targets) Private Endpoints/Private Link verwenden.
- **ExpressRoute vs VPN:** ExpressRoute bietet private, deterministische Routing-Pfade und bessere Governance; VPN bleibt kostengünstiger, aber stärker internetabhängig.
- **DDoS Protection:** Für das öffentliche App-Gateway und öffentliche IP-Ressourcen mindestens DDoS IP Protection, idealerweise DDoS Network Protection mit Telemetrie-Integration.
- **Network Watcher:** NSG Flow Logs, Traffic Analytics, Connection Troubleshoot und Packet Capture für Security Investigations aktivieren.

9.2 Betriebssystemebene

- **CIS Benchmark:** Windows Server 2022/2019 Member Server Baseline und separate DC-Baseline anwenden; Abweichungen dokumentieren.
- **Credential Guard / LSA Protection:** Aktivieren, um Credential Theft zu erschweren. `RunAsPPL=1` für LSA Protection; Credential Guard per GPO/Intune/MDM oder Security Baseline.
- **ASR Rules:** Block Office Child Processes, Block Credential Stealing from LSASS, Block PSExec/WMI Prozess-Kaskaden, Attack Surface Reduction im Audit- dann Block-Modus.
- **Windows Firewall:** Tier-spezifische Inbound-Regeln; keine breiten “Any-Any Internal” Ausnahmen.
- **BitLocker + ADE:** OS- und Datendisks mit BitLocker/Azure Disk Encryption oder serverseitiger Verschlüsselung plus Guest-State Controls schützen.

- **Feature Reduktion:** Nicht benötigte Rollen/Features deinstallieren, SMBv1 deaktivieren, Druckdienste, Telnet Client, alte .NET-Komponenten nur bei zwingender Abhängigkeit.
- **PowerShell Logging:** Script Block Logging, Module Logging, Transcription und Protected Event Logging aktivieren.

WINDOWS HARDENING – BEISPIEL

```
# LSA Protection
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" `
  -Name "RunAsPPL" -PropertyType DWord -Value 1 -Force

# SMBv1 deaktivieren
Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol -NoRestart

# PowerShell Script Block Logging
New-Item -Path
"HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging" -Force
New-ItemProperty -Path
"HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging" `
  -Name EnableScriptBlockLogging -PropertyType DWord -Value 1 -Force
```

9.3 SharePoint-Ebene

- **MinRole:** Rollen nicht “kreativ” vermischen. WFE, APP und Search sauber getrennt; Central Admin nur intern, vorzugsweise auf dediziertem APP-Knoten.
- **Managed Accounts:** gMSA für Web App Pools, Search Services und SQL-Dienste, sofern unterstützt; keine statischen, interaktiv nutzbaren Servicekonten.
- **Service Applications:** Eigene App Pools pro Sicherheitsdomäne (z. B. Search, User Profile, Workflow, Secure Store). Keine Sammel-App-Pools.
- **Permission Levels:** Gefährliche Rechte wie `Add and Customize Pages`, `Manage Web`, `Enumerate Permissions` restriktiv vergeben.
- **IRM / AIP:** Sensible Bibliotheken mit Purview Information Protection / IRM koppeln; verhindert unkontrolliertes Offline-Weiterverteilen.
- **Blob Cache:** Keine sensitiven Dokumente anonym oder zu lang gecacht; Dateitypen-Whitelist, TTL und Pfade prüfen.
- **ViewFormPagesLockDown:** Für nicht voll vertrauenswürdige Benutzer aktiv; reduziert Ausführung benutzerdefinierter Seiteninhalte.
- **Browser File Handling:** `Strict`; verhindert unnötiges Inline-Rendering riskanter Dateitypen.
- **Custom Errors:** Keine Stack Traces an Endbenutzer; Diagnose über Correlation IDs und zentrales Logging.

- **STS Security:** Token Signing Zertifikate lifecycle-managed, Token Lifetimes nicht überdehnt, OAuth over HTTP strikt untersagen.
- **Farm Passphrase:** In PAM/Secrets Vault verwalten; Rotation in definierten Wartungsfenstern.

SHAREPOINT HARDENING – AUSZÜGE

```
# Browser File Handling auf Strict setzen
$wa = Get-SPWebApplication "https://intranet.hausfeld.com"
$wa.BrowserFileHandling = "Strict"
$wa.Update()

# ViewFormPagesLockDown aktivieren
Enable-SPFeature -Identity "ViewFormPagesLockDown" -Url
"https://portal.hausfeld.com"

# Site Collection Audit einschalten
$site = Get-SPSite "https://portal.hausfeld.com"
$site.Audit.AuditFlags =
"CheckIn,CheckOut,Delete,Move,Copy,Search,SecurityChange,Update"
$site.Audit.Update()
```

9.4 Datenbankebene

- **SQL Always On Encryption:** TLS für Clientverbindungen und Replikationspfade; Zertifikatsmanagement automatisieren.
- **TDE:** Content DBs, Config DB, Service App DBs und Search-relevante Datenbanken verschlüsseln.
- **SQL Server Audit:** Login Failures, Role Changes, Sensitive SELECTs auf Security-/Config-Objekten, Backup/Restore Events.
- **Least Privilege:** SharePoint-Konten erhalten nur die tatsächlich erforderlichen Server- und DB-Rechte. Kein lokaler Administrator auf SQL-Knoten für SharePoint Service Accounts.
- **Disable Surface Area:** `xp_cmdshell`, OLE Automation, unnötiges CLR, SQL Browser nach Möglichkeit deaktivieren.
- **Network Configuration:** Hidden Instance, kein Public IP, Listener nur intern, Windows Firewall exakt beschränkt.

T-SQL – SURFACE AREA REDUZIEREN

```
EXEC sp_configure 'show advanced options', 1;
RECONFIGURE;
EXEC sp_configure 'xp_cmdshell', 0;
```

```
EXEC sp_configure 'Ole Automation Procedures', 0;
EXEC sp_configure 'clr enabled', 0;
RECONFIGURE;

-- TDE Beispiel (vereinfachter Auszug)
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'Use-Enterprise-Managed-Secret';
CREATE CERTIFICATE HausfeldTDECert WITH SUBJECT = 'TDE for SharePoint DBs';
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_256
ENCRYPTION BY SERVER CERTIFICATE HausfeldTDECert;
```

9.5 Identitäts- und Zugriffsebene

- **Conditional Access:** MFA für alle interaktiven Zugriffe, strenger für externe Sales Consultants; Länder-/Risiko-/Gerätezustand-basiert.
- **PAW:** SharePoint-, SQL-, AD- und Azure-Administratoren verwalten nur von gehärteten Privileged Access Workstations aus.
- **JIT VM Access:** Microsoft Defender for Cloud JIT für RDP/WinRM; Freigaben zeitlich begrenzt und ticketgebunden.
- **PIM:** Azure Rollen, Gruppen und privilegierte Entra Rollen just-in-time aktivieren; keine permanenten Global-/Privileged Role Admins.
- **Service Accounts:** gMSA, Deny Interactive Logon, Deny RDP Logon, random lange Key Material Rotation.
- **Access Reviews:** Externe Berater-Gruppen, Site Collection Admins, Farm Admins, SQL Sysadmins und Bastion-User quartalsweise prüfen.

JEA – EINGESCHRÄNKTER ADMIN ENDPUNKT

```
New-PSRoleCapabilityFile -Path "C:\Program
Files\WindowsPowerShell\Modules\Hausfeld.SP.Admin\RoleCapabilities\SharePointOps.psr
c"
New-PSSessionConfigurationFile -Path "C:\JEA\SharePointOps.pssc" `
  -SessionType RestrictedRemoteServer `
  -RunAsVirtualAccount `
  -RoleDefinitions @{ "HAUSFELD\SP-Operators" = @{ RoleCapabilities =
"SharePointOps" } }
Register-PSSessionConfiguration -Name "SharePointOps" -Path
"C:\JEA\SharePointOps.pssc"
```

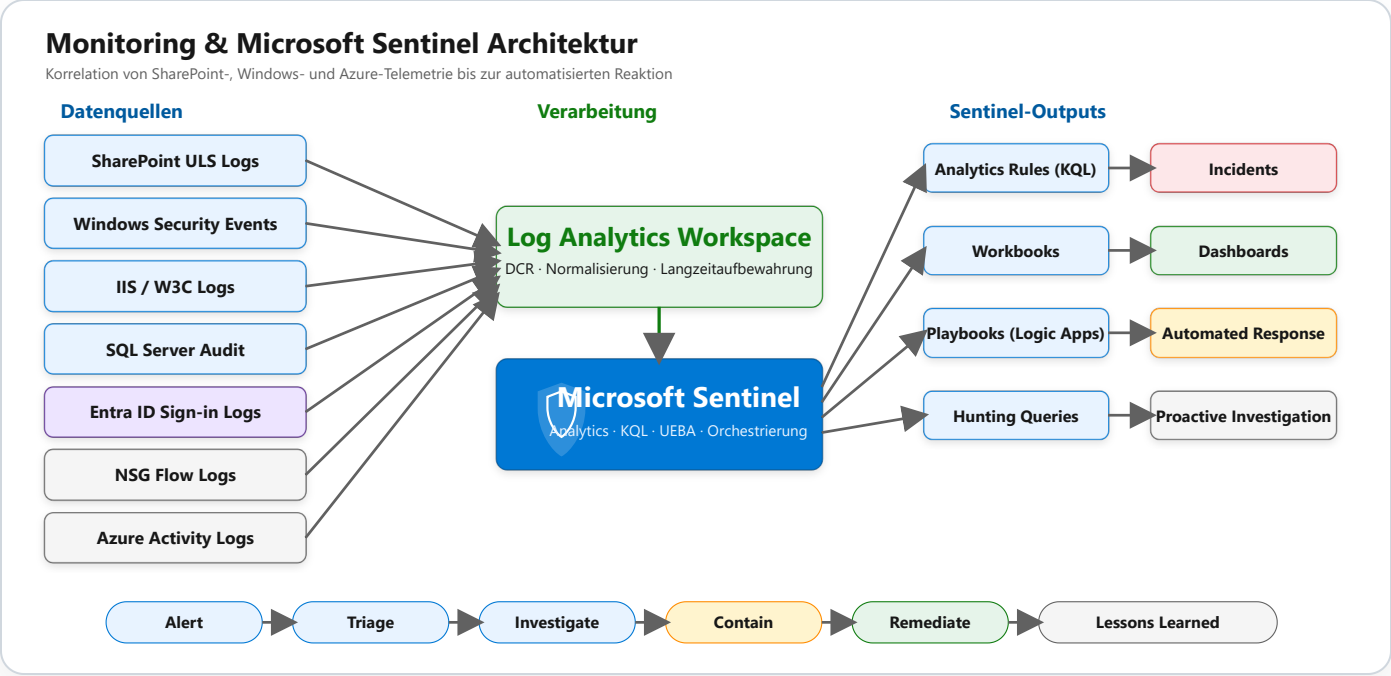
9.6 Datenschutz und Compliance

- **Purview Information Protection:** Labels für HR, R&D, Vertriebsdokumente, Produktspezifikationen und Compliance-Workflows.
- **DLP:** Erkennung von IBAN, Steuer-ID, HR-Daten, Vertragsnummern, Stücklisten und Preislisten in SharePoint-Inhalten.
- **Retention Policies:** Juristisch relevante Inhalte revisionssicher halten; automatische Aufbewahrungslabels für Vertrags- und HR-Bibliotheken.
- **eDiscovery:** Rollenmodell sauber trennen; keine Vollzugriffe ohne Vier-Augen-Prinzip.
- **GDPR:** Datenminimierung, Zugriff auf personenbezogene Daten, Löschkonzepte, Protokollierung von Administratorzugriffen und Drittland-Bewertung für externe Beraterzugriffe beachten.

10. Missbrauchserkennung und Monitoring ▼

10. Missbrauchserkennung und Monitoring

Abbildung 7: Monitoring- und Microsoft-Sentinel-Datenfluss



10.1 Microsoft Sentinel Integration

- **Log Analytics Workspace:** Dediziertes Workspace für Kollaborationsplattformen oder zentraler Security Workspace mit klarer Data Collection Rule (DCR).

- **Data Connectors:** Windows Security Events, Sysmon (empfohlen), Defender for Endpoint, Azure Activity, Entra Sign-in Logs, NSG Flow Logs, Custom Tables für ULS/SharePoint Audit.
- **ULS Ingestion:** AMA/Log Collector oder Filebeat-artige Ingestion in Custom Table `SPULS_CL`. Spalten: `CorrelationId`, `Area`, `Category`, `Level`, `Message`, `Server`.
- **Workbooks:** Dashboards für AuthN-Methoden, NTLM vs Kerberos, Bulk Downloads, Failed Logons, WAF Blocks, Service Account Activity.
- **Playbooks:** Bei High-Confidence Alerts automatisiert: JIT schließen, Benutzer sperren, App Gateway WAF Rule erhöhen, Incident erzeugen, Forensik-VM isolieren.

10.2 ULS Logging

- **Sicherheitsrelevante Kategorien:** Claims Authentication, Security Token Service, PowerShell, SharePoint Foundation General, Database, Search, Workflow Infrastructure, Distributed Cache.
- **Log Levels:** Für Dauerbetrieb `Medium` bzw. gezielt erhöhte Verbosity für Security-relevante Kategorien; Full Verbose nur zeitlich begrenzt.
- **Zentralisierung:** ULS nicht nur lokal belassen; Korrelation über Servergrenzen ist im Incident essenziell.
- **Event Identifiers:** ULS arbeitet primär mit Correlation IDs, Area und Category; zusätzlich sollten verwandte Application Events wie `6398`, `6482`, `7076` mitgeführt werden.

10.3 Windows Security Event Logs

Besonders relevant: `4624`, `4625`, `4648`, `4672`, `4688`, `4768`, `4769`, `4771`, `4776`, sowie PowerShell `4103` und `4104`. Logon Types 2, 3, 8 und 10 sind gesondert auszuwerten; Servicekonten sollten keine interaktiven Logons erzeugen.

10.4 SharePoint Audit Logging

- Site Collection Audit aktivieren und zentral auswerten.
- Dokumentzugriffe, Downloads, Permission Changes, Delete/Restore, Search Queries und Administrative Changes erfassen.
- Exfiltration erkennt man selten an einem einzelnen Download, sondern an Volumen, Entropie, Uhrzeit, IP und Inhaltstyp.

10.5 KQL-Abfragen für Bedrohungserkennung

> **Tabellenannahmen**

> Die Beispiele nutzen Standardtabellen wie `SecurityEvent`, `SigninLogs`, `AzureDiagnostics` sowie Custom Tables `SharePointAuditLog_CL` und `SPULS_CL`.

KQL 1 – BRUTE FORCE DETECTION

```
SecurityEvent
| where EventID == 4625
| where Computer has "SP-WFE"
| summarize FailedAttempts = count() by TargetAccount, IpAddress, bin(TimeGenerated,
5m)
| where FailedAttempts > 10
| project TimeGenerated, TargetAccount, IpAddress, FailedAttempts
```

KQL 2 – UNUSUAL BULK DOWNLOAD DETECTION

```
SharePointAuditLog_CL
| where Operation_s == "FileDownloaded"
| summarize DownloadCount = count(), TotalSizeMB = sum(toint(FileSize_d)) / 1024 /
1024
          by UserId_s, SiteUrl_s, bin(TimeGenerated, 1h)
| where DownloadCount > 50 or TotalSizeMB > 500
| order by DownloadCount desc
```

KQL 3 – PERMISSION ELEVATION DETECTION

```
SharePointAuditLog_CL
| where Operation_s in ("RoleAssignmentAdd","RoleDefinitionAdd","SecurityChange")
| project TimeGenerated, UserId_s, SiteUrl_s, Operation_s, ObjectId_s, Details_s
| order by TimeGenerated desc
```

KQL 4 – AFTER-HOURS ACCESS PATTERNS

```
SharePointAuditLog_CL
| where Operation_s in ("FileAccessed","FileDownloaded","PageViewed")
| extend Hour = datetime_part("hour", TimeGenerated)
| where Hour < 6 or Hour > 21
| summarize Events = count() by UserId_s, bin(TimeGenerated, 1h), SiteUrl_s
| where Events > 25
```

KQL 5 – NTLM USAGE DETECTION

```
SecurityEvent
| where EventID == 4624
| where AuthenticationPackageName =~ "NTLM"
| where Computer has_any ("SP-WFE","SP-APP","SQL-AG")
| summarize Count = count() by Computer, TargetAccount, IpAddress, LogonType,
bin(TimeGenerated, 1h)
| order by Count desc
```

KQL 6 – FAILED KERBEROS AUTHENTICATION

```
SecurityEvent
| where EventID in (4768, 4771)
| summarize Failures = count() by TargetAccount, IpAddress, FailureCode,
bin(TimeGenerated, 15m)
| where Failures > 5
| order by Failures desc
```

KQL 7 – SERVICE ACCOUNT MISUSE

```
SecurityEvent
| where EventID == 4624
| where TargetAccount endswith "$" == false
| where TargetAccount in~
("HAUSFELD\\sp_farm","HAUSFELD\\sp_web","HAUSFELD\\sqlsvc","HAUSFELD\\sp_search")
| where LogonType in (2, 10)
| project TimeGenerated, Computer, TargetAccount, IpAddress, LogonType
```

KQL 8 – LATERAL MOVEMENT INDICATORS

```
SecurityEvent
| where EventID in (4624, 4648, 4688)
| where Computer has_any ("SP-WFE","SP-APP","SP-SRCH","SQL-AG")
| where Process has_any ("psexec", "wmic", "winrs", "wsmprovhost", "powershell.exe")
   or CommandLine has_any ("Invoke-Command", "Enter-PSSession", "schtasks", "\\\\")
| project TimeGenerated, Computer, Account, Process, CommandLine, IpAddress
```

KQL 9 – DATA EXFILTRATION PATTERN

```
SharePointAuditLog_CL
| where Operation_s == "FileDownloaded"
```

```
| summarize Files = count(), Sites = dcount(SiteUrl_s), Libraries =
dcount(Library_s)
          by UserId_s, ClientIP_s, bin(TimeGenerated, 30m)
| where Files > 100 and Sites > 3
| order by Files desc
```

KQL 10 – EXTERNAL ACCESS ANOMALIES

```
SigninLogs
| where AppDisplayName has "SharePoint"
| where UserType =~ "Guest" or UserPrincipalName has "consultant"
| summarize Countries = make_set(LocationDetails.countryOrRegion), Signins = count()
          by UserPrincipalName, bin(TimeGenerated, 1d)
| where array_length(Countries) > 2 or Signins > 30
```

KQL 11 – WAF BLOCKS AGAINST LEGACY ENDPOINTS

```
AzureDiagnostics
| where ResourceType == "APPLICATIONGATEWAYS"
| where requestUri_s has_any ("/_vti_bin/", "/_api/", "/_layouts/")
| where action_s in ("Blocked", "Detected")
| summarize Hits = count() by clientIP_s, requestUri_s, ruleId_s, bin(TimeGenerated,
15m)
| order by Hits desc
```

KQL 12 – ULS SECURITY ERROR CORRELATION

```
SPULS_CL
| where Area_s in ("Claims Authentication","Security Token Service","SharePoint
Foundation")
| where Level_s in ("Unexpected","Monitorable")
| where Message has_any ("Access denied", "NTLM", "Kerberos", "token", "digest",
"relay")
| project TimeGenerated, Server_s, Area_s, Category_s, CorrelationId_g, Message
```

10.6 Incident Response Playbooks

Containment

- Kompromittierten User/Service Account sofort sperren oder Passwort/gMSA Key rotieren.
- JIT/RDP/WinRM schließen; betroffene VM per NSG/ASG isolieren.
- Bei Web-Angriffen WAF Custom Rule auf IOC/IP/User-Agent verschärfen.

Evidence Preservation

- ULS, IIS, Security Logs, Sysmon, App Gateway Logs, NSG Flow Logs sichern.
- Memory Capture und Disk Snapshot der betroffenen VM nach DFIR-Freigabe.
- Correlation IDs, Ticketnummern, Zeitquellen und Admin-Aktivierungen dokumentieren.

Recovery

- Patchstand verifizieren, Secrets rotieren, SPNs/Delegation prüfen.
- Farm Health Analyzer, Search Topology, SQL Integrity und Content Konsistenz validieren.
- Wiederfreigabe nur nach abgeschlossener Root-Cause-Analyse.

SharePoint-spezifische IR-Schritte

- Auditieren, welche Site Collections und Bibliotheken betroffen sind.
- App Catalog, Solutions, Features, Timer Jobs und Web.Config-Diffs prüfen.
- STS-Zertifikate, Trusted Token Issuer und OAuth Trusts auf Manipulation prüfen.

11. Maßnahmenkatalog und Priorisierung

11. Maßnahmenkatalog und Priorisierung

Zeithorizont	Maßnahme	Aufwand	Verantwortlich	Erwartete Risikoreduktion
Sofort (0–2 Wochen)	NTLM-Nutzung auditieren; Public IPs auf Farm-VMs entfernen; WAF in Prevention Mode; fehlende SPSE/Windows/SQL Security Updates einspielen.	Mittel	SharePoint Platform + Azure Network + Windows	Sehr hoch – reduziert R1, R4, R5 unmittelbar.
Sofort (0–2 Wochen)	Central Admin und WinRM nur aus Management-Subnetz/PAW zulassen; JIT aktivieren.	Niedrig	Azure Security + Server Ops	Hoch – senkt Laterale Bewegung und Admin-Missbrauch.
Kurzfristig (2–8 Wochen)	OIDC mit Entra ID für externe Consultants produktiv einführen; MFA und Conditional Access erzwingen.	Hoch	IAM + SharePoint Platform	Sehr hoch – reduziert Credential-Stuffing, FBA-Abhängigkeit und unsichere Extranet-Logons.
Kurzfristig (2–8 Wochen)	SPN-/Kerberos-Bereinigung, gMSA-Einführung, Deny Interactive Logon für Service Accounts.	Mittel	AD/IAM + SharePoint Platform + DBA	Hoch – reduziert NTLM-Fallback, Kerberoasting-Risiko und Servicekonto-Missbrauch.
Kurzfristig (2–8 Wochen)	SOAP/ASMX und unnötiges WebDAV inventarisieren und abschalten; Browser File Handling auf Strict setzen.	Mittel	SharePoint Platform	Hoch – verkleinert exposed surface deutlich.
Mittelfristig (2–6 Monate)	Sentinel Use Cases, ULS-Ingestion, KQL-Detections, Workbooks	Hoch	SOC + Platform Engineering	Hoch – verbessert Detection/Response und forensische Tiefe.

Zeithorizont	Maßnahme	Aufwand	Verantwortlich	Erwartete Risikoreduktion
	und Playbooks produktionsreif machen.			
Mittelfristig (2–6 Monate)	SQL TDE, Audit, TLS Enforcement, Surface Area Reduction, Backup/Restore-Härtung.	Mittel	DBA Team	Hoch – schützt Content-, Config- und Search-Daten.
Mittelfristig (2–6 Monate)	JEA/Constrained Language Mode für SharePoint-Administration; vollständige PAW-Pflicht.	Mittel	Server Ops + Security Engineering	Mittel bis hoch – reduziert Admin-Abuse und Remote Shell Missbrauch.
Langfristig (6–12 Monate)	Architekturreview für weitere Entkopplung von Legacy-Customizations, Workflow-Altlasten und Suche nach Zero-Trust-konformen Publishing-Modellen.	Hoch	Enterprise Architecture + SharePoint Product Owner	Strategisch sehr hoch – reduziert technische Schuld.
Langfristig (6–12 Monate)	Compliance-Integration mit Purview Labels, DLP, eDiscovery und regelmäßigen Access Reviews konsolidieren.	Mittel	Compliance + IAM + Collaboration	Mittel – stärkt Datenschutz und Governance.

12. Sicherheitsberater-Frageliste

12. Sicherheitsberater-Frageliste

Die folgende Sicherheitsberater-Frageliste dient als systematische Checkliste für Security Consultants, um die SharePoint Subscription Edition Farm der Hausfeld Gruppe in Azure IaaS strukturiert zu bewerten. Sie bündelt Identität, Netzwerk, Farm-Konfiguration, SQL, Härtung, Monitoring, Recovery, Governance, Lifecycle und externe Zugriffe in prüfbare Leitfragen mit Soll-Zustand, Risiko und Verweispunkten.

Jede Antwort sollte mit belastbaren Nachweisen hinterlegt werden, z. B. Azure-Konfigurationen, GPO-Exports, SharePoint PowerShell-Ausgaben, SQL-Auditdaten, Sentinel-Abfragen oder dokumentierten Betriebsprozessen.

64	10	22	26	16
Fragen gesamt	Kategorien	Kritische Prüfpunkte	Wichtige Prüfpunkte	Standard-Prüfpunkte

Alle Antworten öffnen | Alle Antworten schließen

A – Identität & Authentifizierung

8 Fragen · Bewertung der Authentifizierungsarchitektur und Identity Governance

A.01 Welches primäre Authentifizierungsprotokoll wird für Benutzeranmeldungen an SharePoint verwendet? ▸

A.02 Ist NTLM auf allen Farm-Servern (WFE, APP, SQL) vollständig deaktiviert oder zumindest auditiert? ▸

A.03 Sind alle SharePoint-relevanten Service Principal Names (SPNs) korrekt und duplikatfrei konfiguriert? ▸

A.04 Werden Group Managed Service Accounts (gMSA) für alle SharePoint- und SQL-Dienste verwendet? ▸

A.05 Ist Multi-Faktor-Authentifizierung (MFA) für alle Benutzergruppen aktiviert – insbesondere für externe Sales Consultants? ▸

A.06 Welche Kerberos-Delegationstypen sind für SharePoint-Servicekonten konfiguriert? ▸

A.07 Wie werden privilegierte Administratorkonten (Farm Admin, Site Collection Admin, SQL sysadmin) geschützt? ▸

A.08 Existiert ein regelmäßiger Access Review für privilegierte Rollen und externe Benutzer? ▸

B – Netzwerk & Infrastruktur

8 Fragen · Prüfung von Netzwerksegmentierung, Konnektivität und Exposition

B.01 Ist das Azure VNet in dedizierte Subnetze pro Tier (AppGW, WFE, APP, Search, SQL, Management, Identity) segmentiert? ▸

B.02 Sind Network Security Groups (NSGs) nach dem Least-Privilege-Prinzip konfiguriert mit expliziter Deny-All-Abschlussregel? ▸

B.03 Wird ein Azure Application Gateway mit WAF v2 als Reverse Proxy vor den SharePoint Web Front Ends eingesetzt? ▸

B.04 Wie ist die Konnektivität zum Düsseldorfer Hauptstandort und zu den Landesgesellschaften realisiert? ▸

B.05 Haben die SharePoint-VMs öffentliche IP-Adressen? ▸

B.06 Ist JIT (Just-In-Time) VM Access für administrative RDP/WinRM-Zugriffe konfiguriert? ▸

B.07 Werden NSG Flow Logs und Traffic Analytics aktiviert und ausgewertet? ▸

B.08 Ist die SQL-Kommunikation zwischen SharePoint und SQL Server verschlüsselt? ▸

C – SharePoint Farm Konfiguration

8 Fragen · Review der Farmrollen, Legacy-Angriffsflächen und Betriebsparameter

C.01 Sind die MinRoles korrekt konfiguriert und werden keine Rollen vermischt? ▸

C.02 Ist Browser File Handling auf "Strict" gesetzt? ▸

C.03 Sind SOAP/ASMX Legacy Web Services deaktiviert oder zumindest zugriffsbeschränkt? ▸

C.04 Ist WebDAV für externe Benutzer deaktiviert oder auf bestimmte IP-Ranges beschränkt? ▸

C.05 Wie ist die Search-Konfiguration hinsichtlich Security Trimming und Crawl Rules abgesichert? ▸

C.06 Werden SharePoint Designer Workflows oder Legacy Workflow Manager verwendet? ▸

C.07 Ist die Farm Passphrase sicher verwahrt und wird sie regelmäßig rotiert? ▸

C.08 Gibt es benutzerdefinierte Farm Solutions oder Sandboxed Solutions und wie werden diese kontrolliert? ▸

D – SQL Server & Datenbank

6 Fragen · Datenbankschutz, SQL Surface Area und Backup-Härtung

D.01 Ist Transparent Data Encryption (TDE) für alle SharePoint-Datenbanken aktiviert? ▸

D.02 Sind xp_cmdshell, OLE Automation und CLR auf dem SQL Server deaktiviert? ▸

D.03 Welche Rechte haben die SharePoint-Dienstkonten auf SQL-Ebene? ▸

D.04 Ist SQL Server Audit aktiviert und werden Login Failures, Role Changes und Backup-Events erfasst? ▸

D.05 Ist der SQL Browser Service deaktiviert und die SQL-Instanz auf einen festen Port konfiguriert? ▸

D.06 Werden SQL-Backups verschlüsselt und an einem separaten, zugriffsbeschränkten Speicherort abgelegt? ▸

E – Betriebssystem & Server-Härtung

6 Fragen · Betriebssystem-Härtung, Logging und lokale Schutzmechanismen

E.01 Ist Credential Guard und LSA Protection (RunAsPPL) auf allen Farm-Servern aktiviert? ▸

E.02 Sind Attack Surface Reduction (ASR) Rules im Block-Modus aktiv? ▸

E.03 Ist PowerShell Script Block Logging, Module Logging und Transcription aktiviert? ▸

E.04 Ist SMBv1 deaktiviert und SMB Signing erzwungen? ▸

E.05 Werden die Windows Server nach einem CIS Benchmark oder einer vergleichbaren Baseline gehärtet? ▸

E.06 Ist die Windows Firewall mit tier-spezifischen Inbound-Regeln auf allen Servern aktiv? ▸

F – Monitoring, Logging & Incident Response

7 Fragen · Detektion, Telemetrie und Reaktionsfähigkeit des SOC

F.01	Ist Microsoft Sentinel mit allen relevanten Data Connectors für die SharePoint-Umgebung konfiguriert?	▸
F.02	Existieren spezifische Analytics Rules (KQL) für SharePoint-Bedrohungsszenarien?	▸
F.03	Werden ULS-Logs zentralisiert und in das SIEM eingebunden?	▸
F.04	Ist SharePoint Site Collection Audit Logging für alle Site Collections aktiviert?	▸
F.05	Existiert ein dokumentierter Incident Response Plan speziell für SharePoint-Sicherheitsvorfälle?	▸
F.06	Werden Sentinel Workbooks/Dashboards für SharePoint Security Monitoring genutzt?	▸
F.07	Sind automatisierte Playbooks (Logic Apps) für High-Confidence Alerts konfiguriert?	▸

G – Backup, Recovery & Business Continuity

5 Fragen · Backup-, Restore- und Notfallvorsorge für die Farm

G.01	Werden regelmäßige SharePoint Farm-Backups (Full + Differential) durchgeführt und getestet?	▸
G.02	Existiert ein dokumentierter Disaster Recovery Plan für die gesamte SharePoint-Farm?	▸
G.03	Werden die SQL Always On Availability Groups überwacht und ist Automatic Failover konfiguriert?	▸
G.04	Sind die Backup-Speicherorte vom produktiven Netzwerk getrennt und zugriffsbeschränkt?	▸

G.05 Wird die Farm-Konfiguration (IIS Bindings, SPNs, Certificates, DNS, GPOs) dokumentiert und versioniert? ▸

H – Compliance, Datenschutz & Governance

6 Fragen · Datenschutz, Records Management und Governance-Kontrollen

H.01 Sind Microsoft Purview Information Protection Labels für sensible Dokumentkategorien konfiguriert? ▸

H.02 Sind Data Loss Prevention (DLP) Policies für SharePoint-Inhalte aktiv? ▸

H.03 Werden Retention Policies und Labels für rechtlich relevante Inhalte durchgesetzt? ▸

H.04 Wie wird die DSGVO-Konformität für personenbezogene Daten in SharePoint sichergestellt? ▸

H.05 Ist eDiscovery konfiguriert und werden die Zugriffsrechte nach dem Vier-Augen-Prinzip vergeben? ▸

H.06 Werden externe Sales Consultants durch Identity Governance (Lifecycle, Access Reviews, Terms of Use) verwaltet? ▸

I – Patch Management & Lifecycle

5 Fragen · Patch-Prozesse, Staging und Lifecycle-Steuerung

I.01 Werden SharePoint Subscription Edition Public Updates (PUs) zeitnah eingespielt? ▸

I.02 Werden Windows Server Updates und SQL Server Cumulative Updates regelmäßig eingespielt? ▸

I.03 Gibt es eine Staging-/Test-Umgebung für Patches bevor sie in die Produktion gehen? ▸

I.04	Werden Third-Party-Komponenten (z.B. PDF-Viewer, Antivirus, Monitoring Agents) ebenfalls gepatcht?	▸
I.05	Ist der End-of-Support-Zeitplan für alle eingesetzten Komponenten bekannt und geplant?	▸

J – Externe Zugriffe & Partnerintegration

5 Fragen · Externer Zugriff, Geräteschutz und Offboarding von Partnern

J.01	Wie greifen externe Sales Consultants auf SharePoint zu – über welchen Authentifizierungspfad und welches Gerät?	▸
J.02	Werden die Geräte externer Consultants durch MDM/MAM kontrolliert oder gibt es zumindest App Protection Policies?	▸
J.03	Ist der externe Zugriff auf bestimmte Site Collections, Bibliotheken oder Datenklassen beschränkt?	▸
J.04	Werden Conditional Access Policies mit Standort-, Risiko- und Gerätefiltern für externe Zugriffe angewendet?	▸
J.05	Existiert ein automatischer Offboarding-Prozess für externe Consultants bei Vertragsende?	▸

13. Referenzen und weiterführende Dokumentation ▾

13. Referenzen und weiterführende Dokumentation

Microsoft Learn

- Security for SharePoint Server
- Overview of MinRole and role-based architecture in SharePoint Servers

- OpenID Connect 1.0 authentication in SharePoint Server Subscription Edition
- Plan administrative and service accounts for SharePoint Server
- Authentication overview for SharePoint Server
- Azure Application Gateway documentation
- Microsoft Sentinel overview
- Just-in-time VM access

CIS Benchmarks

- CIS Benchmarks Home
- CIS Benchmark – Microsoft Windows Server
- CIS Benchmark – Microsoft SQL Server

MITRE ATT&CK

- MITRE ATT&CK
- Enterprise ATT&CK Matrix
- T1190 – Exploit Public-Facing Application
- T1078 – Valid Accounts
- T1003 – OS Credential Dumping
- T1021 – Remote Services

NIST

- NIST SP 800-63 Digital Identity Guidelines
- NIST SP 800-63B – Authentication and Lifecycle Management
- NIST SP 800-61 Rev. 2 – Computer Security Incident Handling Guide

---

BSI

- BSI IT-Grundschutz – Übersicht
- BSI SYS.1.1.2 – Active Directory
- BSI APP.6.3 – SharePoint
- BSI Cyber-Sicherheitsempfehlungen

> **Empfohlene Nutzung des Dokuments**

> Dieses HTML-Dokument ist als Betriebs- und Architektur-Referenz gedacht. Für Audits empfiehlt sich die Ableitung einer separaten Kontrollmatrix (Control ID, Sollzustand, Nachweis, Abweichung, Owner, Due Date) auf Basis der priorisierten Maßnahmen aus Abschnitt 11.

Dokument erstellt für die Hausfeld Gruppe GmbH & Co. KG · SharePoint Subscription Edition auf Azure IaaS · Stand 15.06.2026