Technologiegrundsätze

SAP Managed Services

der

BARMER und der HEK

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Dieses Dokument enthält allgemeine Bestimmungen zu IT-Dienstleistungen und Lösungen, die für den vorliegenden Vertrag gelten. Etwaige spezifische Bestimmungen zur Informationstechnologie sind in **01-03 Technologiedefinitionen** enthalten.

2 Auftraggebernahe und unterstützende Technologie Services

2.1 Technologie Services

„**Technologie Service“** ist die Funktionalität (z.B. Anwendungsfunktionalität, Betriebssystemfunktionalität) einer Technologiekomponente (z.B. Anwendung, Betriebssystem), die der Umgebung (z.B. Benutzer, andere Technologiekomponenten) bereitgestellt wird.

2.2 Auftraggebernahe Technologie Services

Der *Auftragnehmer* wird Technologie Services für die direkte Nutzung durch den *Auftraggeber* bereitstellen und verwalten (z.B. entwerfen, erstellen, betreiben, unterstützen) (zusammenfassend als „Auftraggebernahe Technologie Services“ bezeichnet; jeder einzelne ist ein „Auftraggebernaher Technologie Service“).

Auftraggebernahe Technologie Services sind im **01-02-01 Service Katalog** ausdrücklich aufgeführt und in **01-03 Technologiedefinitionen** soweit erforderlich ergänzend beschrieben.

2.3 Unterstützende Technologie Services

Der *Auftragnehmer* erbringt und verwaltet in vollem Umfang unterstützende Technologie Services nach Stand der Technik (einschließlich Weiterentwicklung aufgrund von Security-Issues oder Supportabkündigungen), die für die ordnungsgemäße Erbringung und Bereitstellung der ausdrücklich beschriebenen auftraggebernahen Technologie Services erforderlich sind oder damit zusammenhängen (die „Unterstützenden Technologie Services“).

3 ITSM-System

3.1 ITSM-System des Auftraggebers

Der *Auftraggeber* verwendet sein eigenes ITSM-System (ITSM) zur Unterstützung von Service-Management-Prozessen. Die Prozesse sind nach ITIL v4 aufgebaut.

Der *Auftragnehmer* ist verpflichtet, sein ITSM-System über eine Rest-API Schnittstelle an das *Auftraggeber* ITSM-System zu koppeln, um die in **02-04 Prozess Richtlinien** definierten Service Lifecycle Management-Prozesse zu erbringen. Sollte der *Auftragnehmer* in Folge eines Verschuldens des *Auftragnehmers* trotzdem über das ITSM-System des *Auftraggebers* arbeiten müssen (sei es, weil der *Auftragnehmer* Schnittstellen nicht rechtzeitig bereitstellt oder in der Transition vor einer ITSM-System Integration die toolgestützte Zusammenarbeit erforderlich wird), sind die daraus resultierenden Mehraufwände und Kosten (z.B. Lizenzkosten) durch den *Auftragnehmer* zu tragen.

3.2 Service Integration

Alle im Rahmen der Vertragserfüllung erstellten (oder erfassten) spezifischen Daten sind Eigentum des *Auftraggebers*. Um die Integrität, die Vollständigkeit der Daten und die Orchestrierung der Dienste und Prozesse zwischen den Dienstleistern zu gewährleisten, wird ein zentrales Service Integration (SI) Toolset genutzt. Dieses Toolset stellt den Master für alle Servicedaten unter

diesem Vertrag dar. Im Mittelpunkt des ITSM-Systems betreibt der *Auftraggeber* die Software ServiceNow.

3.3 ITSM-Integrationsschicht

Der *Auftraggeber* stellt eine ITSM-Integrationsschicht für die technische Kopplung und fachliche Integration des ITSM-Systems (ServiceNow) des *Auftraggebers* und des *Auftragnehmers* bereit. Hierüber wird die technische Kopplung und fachliche Integration des ITSM-Systems des *Auftraggebers* und des ITSM-Systems des *Auftragnehmers* zum Zwecke des Austauschs relevanter Service-Management-Daten hergestellt. Die für einen Konnektor notwendige Netzwerkverbindung wird der *Auftragnehmer* entsprechend der sicherheitstechnischen Anforderung des *Auftraggebers* in diesem Vertrag betreiben.

3.3.1 ITSM-Konnektor

Der *Auftraggeber* erwartet für folgende Prozesse/Praktiken eine technische Kopplung über die oben genannte ITSM-Integrationsschicht:

- Incident Management
- Problem Management
- Change Management
- Konfigurationsmanagement (CMDB)
- Hardware-Asset-Management (HAM)
- Request Management
- Service Katalog Management
- Identity Management (u. a. Übertragung IAM-Daten an Auftragnehmer)
- Event Management
- Financial Management
- Reporting
- Software-Asset-Management

Auf der Grundlage dieser Vereinbarung wird der *Auftragnehmer* einen Zwei-Wege-Konnektor zwischen dem ITSM-System des *Auftragnehmers* und der ITSM-Integrationsschicht des *Auftraggebers* implementieren.

Im Rahmen des Lifecycelmanagements der ITSM-Integrationsschicht durch den *Auftraggeber* sind Anpassungen auf Seiten des *Auftragnehmers* in folgendem Umfang zu berücksichtigen:

- 6 Releases je Kalenderjahr
- Vereinbarte Änderungen in kleinem Umfang (z.B. Zugangsänderungen, Passwort-Changes, Feldänderungen)

Erforderliche Anpassungen darüber hinaus unterliegen den Vereinbarungen analog **02-05 Projektgrundsätze**.

3.3.2 Schnittstellen Definition

Zur Anbindung an das ITSM-System des *Auftraggebers* stehen verschiedene APIs bereit, die standardmäßig aktiv sind. Diese APIs bieten die Möglichkeit, mit verschiedenen Funktionen des ITSM-Systems des *Auftraggebers* in ihrer Anwendung zu interagieren.

Es gilt die gültige Dokumentation zum eingesetzten ServiceNow Release.

3.3.3 Fieldmapping für die ITSM-Prozesse/Praktiken

Der *Auftraggeber* wird für die nachfolgenden ITSM-Prozesse die Pflichtfelder und das jeweilige Statusmodell vorgeben.

- Incident Management
- Problem Management
- Change Management
- Konfigurationsmanagament (CMDB) (je CI-Klassen an der Fachlichkeit auszurichten)
- Hardware-Asset-Management (HAM)
- Request Management
- Service Katalog Management
- Identity Management (u. a. Übertragung IAM-Daten an Auftragnehmer)
- Event Management
- Financial Management
- Reporting (z.B. Berichte, Rohdaten)
- Software-Asset-Management
- Informationen zu den Software-Installationen auf Clients und Servern

3.4 Software-Asset-Management

Auf allen vom *Auftragnehmer* bereitgestellten Systemen (Hardware, virtuell, Cloud-Computing-Dienst) ist eine Software-Scanfunktionalität für eine tagesaktuelle Auswertung vorzusehen. Bei Systemen, die keine Software-Scan-Funktionalität bieten, ist eine externe Betriebsabfrage bereitzustellen. Die Scan-Daten sind im Roh-Format entsprechend Abstimmung zwischen *Auftraggeber* und *Auftragnehmer* im Rahmen der Transition bereitzustellen. Die Normalisierung erfolgt beim *Auftraggeber*.

Im Rahmen der geforderten Anbindung des *Auftragnehmers* an das ITSM-System des *Auftraggebers* (siehe Ziffer 3.1) und der damit verbundenen Kopplung an den ITSM-Konnektor werden folgende Datenlieferungen gefordert:

- Installierte Software auf den Servern (inkl. virtuell) – beinhaltend die Informationen zu installierten Serverbetriebssystemen (Windows, Linux, etc.)
- Software Produkte (Hersteller, Produkt, Edition, Version, Sprache, Servicepack, Hotfix (Semantic Versioning)), Installationsdatum sowie Installationspfad
- Installierte Software auf allen Clients – beinhaltend, sofern vorhanden, Hersteller, Produkt, Edition, Version, Sprache, Servicepack, Hotfix (Semantic Versioning), Installationsdatum sowie Installationspfad.
- Software-Usage. Dieser enthält u.a. anonymisierbar und pseudonymisierbar EU-DSGVO-konforme Darstellung der aufgerufenen Software pro Client mit den Daten - Softwarenamen, ggf. aufgerufen durch Username sowie letztes Aufrufdatum (tagesgenau).

3.5 Konfigurationsmanagement (CMDB)

Für die beim *Auftragnehmer* eingesetzten Systeme sind Informationen zu den technischen Configuration Items (CIs) zu liefern, die auch die Relationen zur Infrastruktur und anderen CIs beinhalten.

Für alle CIs sind Informationen des Betriebsstatus und Lifecycle bei jeder Änderung tagesaktuell zu liefern.

Alle für die Abrechnung relevanten Informationen in den gelieferten CIs sind in den gelieferten Daten mitzuführen.

3.6 Hardware-Asset-Management (HAM)

Der *Auftraggeber* liefert für Hardware, die von Relevanz für den *Auftraggeber* ist, die Daten gemäß Herstellerinformation. Das hat auch die Hersteller-Kenn-Nummern der Hardware (zum Lifecycle-Abgleich über den Content-Service in ServiceNow) zu beinhalten.

Alle für die Abrechnung relevanten Informationen der gelieferten Assets sind in den gelieferten Daten mitzuführen.

Die Hardware-Asset-Daten des *Auftragnehmers* sind in Absprache um Referenzen des *Auftraggebers* anzureichen (z.B. Auftragsnummer, Bestellnummer, Preislistenposition).

4 Monitoring

4.1 Schnittstelle Event-Management

Zur Sicherstellung der vom *Auftragnehmer* verantworteten Services setzt dieser eine Monitoring-Umgebung ein. Die Monitoring-Meldungen (Events) werden im Event-Management verarbeitet.

Jegliche Event Management Tools, die beim *Auftragnehmer* zur Überwachung der zu erbringenden Leistungen für den *Auftraggeber* eingesetzt werden, müssen über eine technische Schnittstelle an das zentrale Event Management des *Auftraggebers* angebunden werden. Insbesondere müssen hier Statuswechselmeldungen (nahe Realtime) an das zentrale Event Management System des *Auftraggebers* zur weiteren Verarbeitung übergeben werden. Auch Leistungskennzahlen aus den von *Auftragnehmer* verantworteten und überwachten Services werden nach Bedarf des *Auftraggebers* in der dann festgelegten Häufigkeit und Formatierung bereitgestellt. Die Anbindung der technischen Schnittstelle übernimmt der *Auftraggeber*, der *Auftragnehmer* hat die Daten über eine geeignete technische Schnittstelle im JSON-Format bereit zu stellen.

4.2 Monitoring Service - Servicekonzept

4.2.1 Einleitung

Grundlage jedes ordnungsgemäßen Betriebs ist das Monitoring verschiedener Parameter eines IT-Services. Der *Auftraggeber* oder ein von ihm beauftragter Dritter betreibt im Rahmen des Betriebs seiner Applikationen ein eigenes Umbrella-Monitoring, das auf Basis aller Monitoring-Daten, der CMDB und weiterer Informationen ein Gesamtbild des Status der Applikationslandschaft generiert und entsprechende Maßnahmen ableitet. Zur Erfüllung dieser Leistungen werden entsprechende Monitoring-Daten benötigt (z.B. qualifizierte Events mit den darin integrierten Rohdaten). Daher ist der *Auftragnehmer* verpflichtet, dem *Auftraggeber* im Rahmen des Measuring & Monitorings erhobene Daten unverzüglich (nahe Echtzeit) über entsprechende Schnittstellen zur Verfügung zu stellen.

4.2.2 Allgemeine Anforderungen

4.2.3 IT-Service-Monitoring

Der *Auftragnehmer* betreibt zur Erbringung der unter diesen Vertrag vereinbarten Services ein regelmäßiges, toolgestütztes Measuring & Monitoring der Dienste und technischen Parameter. Das Service-Monitoring umfasst hierbei alle automatisierten Überwachungstätigkeiten des *Auftragnehmers*, die zur Sicherstellung der vereinbarten Leistungen, Service-Level-Targets und KPIs

notwendig sind. Ergänzend werden Informationen erhoben, die die IT-Service-Management-Prozesse (z.B. Capacity- Management, Event-Management, Incident-Management) benötigen.

Alle Monitoring-Informationen laufen an einer zentralen Stelle des *Auftragnehmers* auf, der auf Basis der eingehenden Daten den Status der jeweiligen IT-Services darstellt und auf dessen Basis automatisiert oder manuell entsprechende Maßnahmen (im Sinne der relevanten Prozesse, insb. des Incident Managements und Problem Managements) einleiten wird. Das IT-Service-Monitoring wird für alle IT-Services, die durch den *Auftragnehmer* in Rahmen dieses Vertrags verantwortet werden, erbracht.

Sofern die Notwendigkeit besteht, dass der *Auftraggeber* direkt Systeme auf Ebene der Auftragnehmer-Verantwortung abfragt, erfolgt die Abfrage in den gleichen Intervallen, die der *Auftragnehmer* für seinen ordnungsgemäßen Betrieb nutzt.

4.2.4 Monitoring-Daten-Provisionierung

Der *Auftragnehmer* stellt für das Umbrella-Monitoring des *Auftraggebers* in Abstimmung mit dem *Auftraggeber* alle benötigten Daten aus dem Service-Monitoring über eine im Rahmen der Transition definierten Schnittstelle unverzüglich (nahe Echtzeit) in einem definierten und abgestimmten Format (qualifizierte Events mit den darin integrierten Rohdaten) zur Verfügung.

Neben der Bereitstellung von Log-Daten für das Umbrella-Monitoring des *Auftraggebers* sendet der *Auftragnehmer* nach Abstimmung zwischen den Parteien entsprechende Meldungen an einen Syslog Server des *Auftraggebers* oder einen von ihm beauftragten Dritte.

4.2.5 Umgebungsspezifische Monitoring-Anforderungen

Der *Auftragnehmer* betreibt für das Monitoring eigene Umgebungen, die gemäß der Datenschutz- und Sicherheitsrichtlinien getrennt betrieben werden. Hierbei ist es möglich, die Monitoring-Daten auszuleiten und zentral zu verarbeiten.

4.2.6 Monitoring-Agenten

Im Rahmen des Betriebes nutzt der *Auftraggeber* eigene Monitoring-Systeme.

Der *Auftraggeber* erhält die uneingeschränkte Möglichkeit, eigene Agenten und Technologien zum Monitoren der Komponenten, Anwendungen und Services auf den durch den Auftragnehmer für den Auftraggeber bereitgestellten Systemen zu etablieren. Der *Auftragnehmer* unterstützt den *Auftraggeber* bei der automatisierten Installation sowie Konfiguration der Agententechnologien. Lizenzen für die vom *Auftraggeber* eingesetzten Agenten werden vom *Auftraggeber* bereitgestellt.

4.2.7 Technische Parameter

Die durch den *Auftraggeber* bereitgestellte Schnittstelle zum Empfang der Monitoring-Daten (Events -> Monitoring und Eventmanagement) wird in der Transition vom *Auftragnehmer* zur Übertragung eingebunden.

4.2.8 Betriebsmodell

Es ist sicherzustellen, dass die Monitoring-Umgebungen beim *Auftragnehmer* gemäß den vorgegebenen sicherheitstechnischen und datenschutzrechtlichen Standards und Vorschriften betrieben werden (siehe Anlage **02-09-03 AVV TOMs Informationssicherheit**).

5 Agenten und Softwareverteilung

Der *Auftraggeber* behält sich vor, ein zentrales und skalierbares System zur automatisierten und sicheren Verteilung von Softwarepaketen sowie zur Konfiguration von Servern und Clients beizustellen.

6 Kollaborationstools

Der *Auftragnehmer* arbeitet ausschließlich in den Kollaborationswerkzeugen des *Auftraggebers*, sofern für die Zusammenarbeit keine Toolkopplung vereinbart wurde. U.a. betrifft das:

- Projektplanungswerkzeug
- Testmanagement Tools
- Ressourcenplanung / Ressourcenmanagement / Kapazitäts-Management
- Umgebung für betriebliche Dokumentation (inkl. *Service Management und Governance Handbuch*)
- Dateiablage-Tool
- Kommunikationstools (z.B. Chat, VoIP)
- Berichtswesen

Aktuell setzt der *Auftraggeber* in diesem Umfeld die Atlassian Produkte Jira (inkl. X-Ray für Testmanagement) und Confluence ein. Weiter kommt MS Teams zur Zusammenarbeit (samt damit einhergehend MS Sharepoint Online) zum Einsatz.

Der *Auftraggeber* stellt dem *Auftragnehmer* keine Lizenzen zur Nutzung von MS Teams zur Verfügung. In Folge stellt der *Auftragnehmer* sicher, dass alle Mitarbeitenden des *Auftragnehmers,* die auf die MS Teams Umgebung des *Auftraggebers* zugreifen sollen, hierzu in der Lage sind. Dies bedingt u.a. die Ausstattung mit den entsprechend notwendigen Lizenzen und Zugängen.

Abweichend gilt für die HEK:

Aktuell hat die HEK kein entsprechendes Tool im Einsatz, prüft jedoch derzeit verschiedene Optionen. Über die Form der Zusammenarbeit stimmen sich die HEK und der *Auftragnehmer* während der Transition ab.

7 Cyber Security

Der *Auftraggeber* setzt umfangreiche technologische und organisatorische Maßnahmen zur Erkennung und Abwehr von Gefährdungen ein. Im Folgenden werden Anforderungen an den *Auftragnehmer* beschrieben, welche für die Gewährleistung der IT-Sicherheit des *Auftraggebers* zu erfüllen sind. Die im Folgenden unter dieser Ziffer 7 aufgeführten Anforderungen werden in der Transition zwischen *Auftraggeber* und *Auftragnehmer* hinsichtlich ihrer konkreten Umsetzung abgestimmt und detailliert.

Folgende Übersicht zeigt die geplante IT-Sicherheitsarchitektur der BARMER und HEK in der Übersicht:

Die Übersicht wird bei der Aufforderung zum indikativen Angebot zur Verfügung gestellt.

Abbildung 1 BARMER - Auftraggeber IT-Sicherheitsarchitektur

Die Übersicht wird bei der Aufforderung zum indikativen Angebot zur Verfügung gestellt.

Abbildung 2: HEK - Auftraggeber IT-Sicherheitsarchitektur

Wie skizziert, sieht der *Auftraggeber* vor, einige IT-Sicherheitsmaßnahmen dezentral beim *Auftragnehmer* zu installieren und betreiben zu lassen, und einige Maßnahmen selbst zu betreiben. In vielerlei Fällen werden Schnittstellen von den dezentral betriebenen Systemen in die zentralen Management-Instanzen des *Auftraggebers* gefordert. Folgende Unterkapitel skizzieren diesen Aufgabenschnitt je übergreifender Sicherheitsmaßnahme:

7.1 Distributed Denial of Service (dDoS) Protection

Betreibt der *Auftragnehmer* für den *Auftraggeber* öffentlich aus dem Internet erreichbare Systeme, sind diese in Abstimmung mit dem *Auftraggeber* über einen zentralen dDoS-Protection-Anbieter oder ein Content-Delivery-Network (CDN) des *Auftraggebers* abzusichern.

Dafür notwendige DNS-Einträge sind durch den *Auftragnehmer*, nach Anforderungen des *Auftraggebers*, zu setzen.

Es ist dem *Auftragnehmer* untersagt, für den *Auftraggeber* betriebene Systeme ohne Absprache mit dem *Auftraggeber* direkt aus dem Internet erreichbar zu machen.

7.2 Endpoint Detection & Response (EDR)

Der *Auftragnehmer* implementiert einen Prozess zur automatisierten Installation der vom *Auftraggeber* bereitgestellten EDR-Agent Software auf den für den *Auftraggeber* bereitgestellten Systemen. Es sind angemessene CPU- und Rechenkapazitäten vorzusehen, um den Betrieb der EDR Agenten zu ermöglichen.

Für den Betrieb der Agenten nötige Freischaltungen an der Netzwerkinfrastruktur (bspw. Netzwerk- oder hostbasierte Firewalls, Proxys, Routing-Infrastrukturen) sind in Abstimmung mit dem *Auftraggeber* umzusetzen.

Der *Auftraggeber* erhält über ausgebrachte EDR-Agenten einen wohldefinierten Katalog an Sofortmaßnahmen, die er im Rahmen des Security Incident Managements sowie des EDR-Betriebes eigenständig ausführen darf. Dieser Katalog wird im Rahmen der Transition zwischen *Auftraggeber* und *Auftragnehmer* abgestimmt und umfasst mindestens:

- Die standardmäßige Einschränkung lauffähiger Prozesse und Programme.
- Die Isolierung einzelner Systeme.
- Das Starten und Stoppen von anlassbezogenen Virenscans.
- Die Pflege von Indicator of Compromises (IoCs).

Vom *Auftragnehmer* detektierte IoCs sind automatisiert und unverzüglich in das EDR-System des *Auftraggebers* zu überführen.

Die auf den *Auftraggeber*-Systemen betriebenen EDR-Agenten sind das führende AV- und EDR-System.

Die Funktionsfähigkeit der EDR-Agenten ist im Change-Management des *Auftragnehmers* zu berücksichtigen.

Es sind durch den *Auftragnehmer* keine eigenen Agenten auf *Auftraggeber*-Systemen auszubringen, die die Funktionsfähigkeit der EDR-Agenten einschränken (bspw. konträre AV-Agents).

7.3 Intrusion Detection- / Prevention System (IDS, IPS)

Der *Auftragnehmer* stellt eine hinreichende, dem Stand der Technik entsprechende Überwachung des Netzwerkverkehrs der für den *Auftraggeber* betriebenen Netzwerke sicher. Dies umfasst:

- den Betrieb von IPS-Modulen an den für den Auftraggeber betriebenen Firewalls.
- den Einsatz eines zentralen IDS- oder IPS-Moduls oder einer anderweitigen Maßnahme, bspw. über einen SPAN-Port, ein Tap-Device oder Endpunkt-Agenten, welches Visibilität in den lateralen Traffic innerhalb von Netzwerksegmenten besitzt.

Für die Angriffserkennung nutzt das vom *Auftragnehmer* betriebene IDS/IPS eine Mischung aus Erkennungsmethoden, wie Signaturen, Heuristiken und ML-basierten Regeln.

Der *Auftraggeber* erhält Zugriff auf die vom IDS/IPS generierten Alarme und Telemetriedaten über eine Echtzeitschnittstelle.

Das IDS/IPS bietet standardisierte Schnittstellen mindestens nach ServiceNow-SecOps, SOAR- und gängige SIEM-Tools.

Für den Betrieb des IDS/IPS nötige Firewallfreischaltungen sind in Abstimmung mit dem *Auftraggeber* umzusetzen.

7.4 Patchmanagement (Schwachstellenmanagement)

Alle für den *Auftraggeber* betriebenen Systeme sind täglich, mindestens aber wöchentlich auf Schwachstellen zu prüfen.

Identifizierte Schwachstellen in Behandlungsverantwortung des *Auftragnehmers* sind im Rahmen folgender Fristen zu behandeln:

Risiko-klasse	CVSS-Range	Behebung innerhalb von
Emergency	7.0 - 10.0 in aktiver Ausnutzung (anhand CISA-KEV-Katalog)	3 Tagen nach Bekanntgabe im CISA-KEV-Katalog
Kritisch	9.0 - 10.0	14 Tagen nach Feststellung
Hoch	7.0 - 8.9	30 Tagen nach Feststellung
Mittel	4.0 - 6.9	60 Tagen nach Feststellung
Gering	0.1 - 3.9	6 Monaten nach Feststellung

Tabelle 1: Fristen für Schwachstellen

Darüber hinaus behält sich der *Auftraggeber* das Recht vor, Schwachstellen unabhängig von ihrem CVSS-Score zu priorisieren, wenn dies für die Gewährleistung der Sicherheit des *Auftraggebers* erforderlich ist.

7.4.1 Bestimmungen bezüglich zukünftiger Veränderungen der Quelldatenbanken

Die *Parteien* vereinbaren, dass sie bei signifikanten Veränderungen (z.B. Einstellung des Angebots) der den Bestimmungen in Ziffer 7.4, sowie den Service Levels S.IF.SO.01 und S.IF.SO.02 in **01-04 Service Levels** zu Grunde gelegten Quellverzeichnissen (z.B. CISA-KEV-Katalog) sich auf eine vergleichbare Alternative hinsichtlich Qualität, Aktualität, Handhabbarkeit und Verfügbarkeit verständigen werden, ohne von einem Vertragsänderungsverfahren Gebrauch zu machen.

7.5 Secure Web Gateway, Cloud App Security Broker, WebProxy

Haben durch den *Auftragnehmer* für den *Auftraggeber* betriebene Systeme die Notwendigkeit, auf das Internet zuzugreifen, ist der Traffic über das zentrale Secure Web Gateway (SWG) des *Auftraggebers* oder ein CDN des *Auftraggebers* zu leiten.

Es ist eine Vertrauensstellung zwischen den für den *Auftraggeber* betriebenen Systemen sowie dem SWG herzustellen, sodass verschlüsselter Traffic inspiziert werden kann.

Durch den *Auftragnehmer* ist im Rahmen der Vertragsleistungen kein eigenes SWG oder ein andersartiger Webproxy zu betreiben, um die korrekte Funktionsweise sicherzustellen.

Es sind ohne Absprache keine direkten Webzugriffe von für den *Auftraggeber* betriebene Systeme auf das Internet zu erlauben. Dies ist technisch sicherzustellen.

7.6 Security Information Event Management System (SIEM)

Der *Auftragnehmer* implementiert einen Prozess zur automatisierten Installation der vom *Auftraggeber* bereitgestellten SIEM-Agent Software auf den für den *Auftraggeber* bereitgestellten Systemen installiert.

Es sind angemessene CPU- und Rechenkapazitäten vorzusehen, um den Betrieb zu ermöglichen.

Für den Betrieb der Agenten nötige Freischaltungen an der Netzwerkinfrastruktur sind in Abstimmung mit dem *Auftraggeber* umzusetzen.

Ist die Installation eines SIEM-Agenten nicht möglich, sind auftretende Systemereignisse über alternative Wege (bspw. und insbesondere Syslog) bereitzustellen.

Der *Auftragnehmer* verpflichtet sich, für alle für den *Auftraggeber* betriebenen Systemklassen Protokollierungskonzepte zu erstellen und sicherzustellen, dass die Protokollierung fortlaufend und fehlerfrei abläuft.

Der *Auftragnehmer* stellt dem *Auftraggeber* die erforderlichen Ressourcen (Compute, Storage, ...) zur Verfügung, um evtl. erforderliche Logdaten-Sammler (oder andere erforderliche, lokale SIEM-Komponenten) zu betreiben.

7.7 SOC Level 1 und Level 2

Der *Auftraggeber* hat das Recht, über einen beauftragten SOC-Dienstleister Incident Triage und Response Prozesse, die die für den *Auftraggeber* betriebene Infrastruktur betreffen, zu starten.

Der *Auftragnehmer* hat alle angewiesenen Schritte zu unternehmen, mögliche falschpositive Meldungen durch Konfigurationsänderungen abzustellen.

Es sind 24/7-besetzte Rufnummern und Verteilerkreise für die Zuarbeit in Vorfallsbehandlungen durch den *Auftragnehmer* zu stellen und mit adäquatem Personal zu besetzen.

7.8 SOC Level 3 und CSIRT

Der *Auftraggeber* hat das Recht, über einen beauftragten Digital Forensic and Incident Response (DFIR) Dienstleister Incident Response und forensische Prozesse, die die für den Auftraggeber betriebene Infrastruktur betreffen, zu starten.

Dazu hat der Auftragnehmer dem vom Auftraggeber beauftragten DFIR-Dienstleister entlang definierter Fristen zuzuarbeiten, angefragte Daten (Dumps, IoCs, Vollabzüge etc.) bereitzustellen und gemeinsam mit dem Auftraggeber an der Aufklärung etwaiger Vorfälle mitzuwirken.

Es sind 24/7-besetzte Rufnummern und Verteilerkreise für die Zuarbeit in Vorfallsbehandlungen durch den Dienstleister zu stellen und mit adäquatem Personal zu besetzen.

7.9 Vulnerabilitymanagement System (VMS)

Der Auftragnehmer prüft alle für den Auftraggeber betriebenen Systeme täglich, mindestens aber wöchentlich, auf technische Verwundbarkeiten und erfüllt dabei folgende Rahmenbedingungen:

- Identifizierte Verwundbarkeiten werden anhand einer laufend aktualisierten Datenbank identifiziert, deren Umfang mindestens die 'National Vulnerability Database' (NVD) des NIST sowie die CISA-KEV-Liste sowie wünschenswert weitere Quellen umfasst.
- Die Überprüfung von Schwachstellen erfolgt mit der notwendigen Transparenz auf den Zielsystemen. Dies kann entweder durch authentifizierte Netzwerkscans oder auf den Zielsystemen installierte Endpunktagenten realisiert werden. Reine Portscans erfüllen dieses Kriterium nicht.

Das vom *Auftragnehmer* genutzte Tool zur Identifizierung von Schwachstellen bietet mindestens Export- und automatisierte Schnittstellenfunktionen zu ServiceNow-SecOps, im CSV-Format sowie über einen REST-Endpunkt.

Der *Auftraggeber* erhält täglich und automatisiert die vom *Auftragnehmer* identifizierten Schwachstellendaten. Diese umfassen mindestens:

- Die im letzten Scan neu identifizierten, geschlossen und wiedereröffneten Schwachstellen.
- Zu den einzelnen Findings mindestens die CVE-ID, die CWE-ID, einen einzigartigen Identifier, die zutreffende IP-Adresse, die zutreffende MAC-Adresse, den zutreffenden Hostnamen, eine Kategorie (bspw. Konfigurationsfehler, OS-Verwundbarkeit etc.), das Datum der erstmaligen Identifizierung, Re-Identifizierung und ggf. Schließung, einen Kurztitel, einen Beschreibungstext, einen Lösungshinweis, den Schweregrad als CVSSv2-Score oder neuer, die Angabe, ob die Verwundbarkeit bereits aktiv ausgenutzt wird durch bösartige Akteure.

7.10 Zentrales Firewall Management (Network Orchestration Tool)

Der *Auftraggeber* erhält das Recht, ein Firewall Management Tool technisch an die für den *Auftraggeber* betriebenen Firewalls & Loadbalancer anzubinden. (unter anderem entsprechend „Abschnitt Firewall“ „Abschnitt Load Balancer“).

Der *Auftraggeber* wird in den Firewall-Changeprozess eingebunden.

Der *Auftraggeber* erhält das Recht, regelmäßig und anlassbezogen Firewallregeln zu prüfen und zu rezertifizieren.

7.11 Web-Application-Firewall (WAF)

Werden vom *Auftragnehmer* für den *Auftraggeber* Systeme betrieben, die aus dem Internet erreichbar sind, sind diese einem besonderem Schutzkonzept zu unterziehen. Dies umfasst insbesondere den Einsatz einer vom *Auftraggeber* bereitgestellten Web-Application-Firewall (s.u.) sowie die Platzierung in einer demilitarisierenden Zone (DMZ).

Durch den *Auftragnehmer* betriebene, öffentlich erreichbare Ressourcen, sind hinter einer WAF zu platzieren, die vom *Auftraggeber* beschafft wurde sowie ggf. durch einen vom *Auftraggeber* beschaffenen Dienstleister betrieben oder über eines vom *Auftraggeber* betriebenen CDNs realisiert wird.

Der *Auftragnehmer* verpflichtet sich, dem *Auftraggeber* spezifische WAF-Regeln für die jeweils abgesicherte Applikation zuzuarbeiten, sodass lediglich zwingend notwendiger Traffic erlaubt wird. Nach Absprache kann der *Auftragnehmer* selber befähigt werden, diese Regeln einzupflegen.

Es ist dem *Auftragnehmer* untersagt, für den *Auftraggeber* betriebene Systeme ohne Absprache mit dem *Auftraggeber* direkt aus dem Internet erreichbar zu machen.

8 Identity and Access Management (IAM)

8.1 Einleitung

Alle vom *Auftragnehmer* für die Leistungserbringung auf den Systemen des *Auftraggebers* benötigten Identitäten (Mitarbeiter des *Auftragnehmers*), Accounts (Entitäten in Ziel-Systemen) und benötigte Berechtigungen (Active Directory Gruppen, Einzelberechtigungen, etc.) werden vom *Auftraggeber* bereitgestellt und verwaltet. Der *Auftragnehmer* muss diese Identitäten, Accounts und Berechtigungen in einem Webshop des *Auftraggebers* bestellen. Die Bestellungen werden vom *Auftraggeber* geprüft und genehmigt. Sämtliche hierfür genutzten Identitäten, Accounts und Berechtigungen unterliegen Re-Zertifizierungs-Richtlinien und werden in regelmäßigen Abständen durch den *Auftraggeber* überprüft, freigegeben und somit verlängert. Im Rahmen der Re-Zertifizierungskampagne nicht freigegebene Identitäten, Accounts oder Berechtigungen werden entweder sofort entzogen oder Accounts und Identitäten deaktiviert und dem Leaver-Prozess des *Auftraggebers* zugeführt.

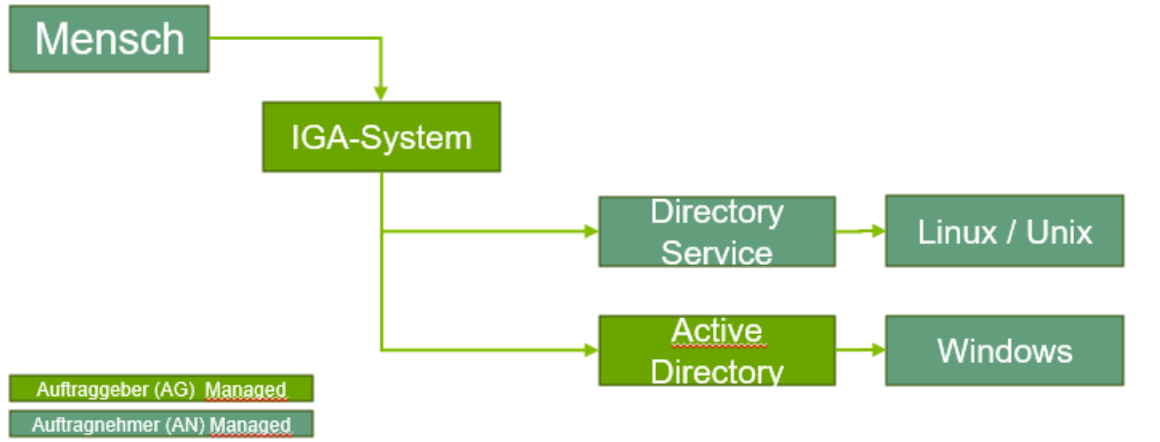

Abbildung 3: Identity and Access Management

8.2 Beigestellte Technologien und Schnittstellen

Zur zentralen Verwaltung aller Identitäten und Accounts stellt der Auftraggeber folgende Technologien zur Verfügung:

- **Identity Governance and Administration (IGA)**

  Das IGA-System basiert auf One Identity zur Abbildung der Prozesse (z.B. Joiner-Mover-Leaver, Re-/Zertifizierung und Bestellung / Genehmigung). Das IGA-System hält ebenfalls alle Schnittstellen, um technische Accounts automatisiert in IAM-Zielsysteme zu provisionieren.

- **Access Management (AM)**

  Der *Auftraggeber* setzt für die Authentifizierung und Autorisierung primär auf Microsoft Active Directory und Active Directory basierte Sub-Services. Accounts werden vom IGA-System direkt darin provisioniert. Sämtliche vom *Auftragnehmer* bereitgestellten und betriebenen Windows-Systeme müssen hieran angebunden werden.

8.3 Übergreifende Rahmenbedingungen

Der *Auftragnehmer* verpflichtet sich im Rahmen seiner Mitwirkungen und Pflichten, dass vorgegebene Rahmenbedingungen eingehalten werden. Dies umfasst u.a. Namenskonventionen, OU-

Strukturen und die verantwortungsvolle Verwendung von Berechtigungen. Detaillierte Vorgaben werden im Rahmen der Ausschreibung in der Transition geteilt.

Nicht zentral verwaltete Accounts (z.B. lokale Accounts) dürfen vom *Auftragnehmer* nur in Ausnahmefällen angelegt und genutzt werden. Diese müssen vorab durch den *Auftraggeber* genehmigt werden.

8.4 Pflichten des Auftragnehmers

8.4.1 Bereitstellung von Systemen

Zur Sicherstellung der Funktionsfähigkeit und Gewährleistung von Redundanz und Performance verpflichtet sich der *Auftragnehmer*, die für die Identity and Access Management Leistungserbringung notwendigen IaaS-/PaaS-Systeme in seiner Umgebung bereit zu stellen.

8.4.2 Linux / Unix Directory Service (DS)

Zur zentralen Verwaltung von Accounts und Berechtigungen für Linux / Unix basierte Systeme muss der *Auftragnehmer* einen Directory Service (LDAP basiert) bereitstellen. In diesem Directory Service dürfen Accounts ausschließlich über das vom *Auftraggeber* bereitgestellte IGA-System angelegt werden. Der *Auftragnehmer* darf hier selbst keine Accounts anlegen. Alle für den *Auftraggeber* betriebenen Linux / Unix Systeme müssen an diesen Directory Service angebunden werden.

Der *Auftragnehmer* stellt sicher, dass die Berechtigungsverwaltung der Unix-/Linux-Systeme über den vom *Auftraggeber* bereitgestellten LDAP-Konnektor technisch umsetzbar ist. Der Betrieb des LDAP-Konnektors obliegt beim *Auftraggeber*.

Zur Vereinfachung der Administration kann der *Auftraggeber* Sprungserver (Jump Server) provisionieren und betreiben. Hierüber kann der *Auftragnehmer* alle von ihm angebotenen Leistungen administrieren. Dazu benötigte Software muss, sofern erforderlich, vom *Auftragnehmer* selbst lizensiert werden. Zugriff auf die entsprechenden Sprungserver muss über das vom *Auftraggeber* bereitgestellte PAM-System erfolgen. Ein entsprechendes Konzept für den Aufbau, den Betrieb und die angedachte Verwendung muss vom *Auftraggeber* genehmigt werden.

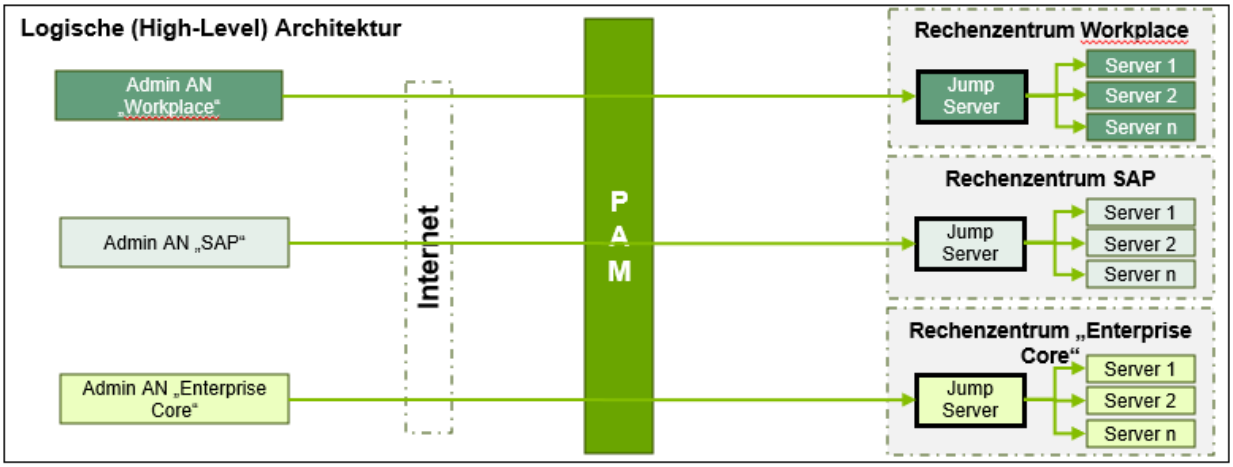

Abbildung 4: Linux / Unix Directory Service

8.4.3 Microsoft Active Directory

Damit der *Auftragnehmer* seine Aufgaben vertragsgemäß ausführen kann, werden ihm eigene Organisationseinheiten (OUs) zugewiesen, die ihm die Durchführung der folgenden Tätigkeiten ermöglichen:

- Administration von Computer-Objekten
- Erstellung und Verwaltung von Group Policies
- Erstellung und Verwaltung von Logon Scripten

8.4.4 Privileged Access Management (PAM)

Der *Auftragnehmer* muss, aufgrund interner und externer Compliance-Vorgaben (siehe **02-09-03 AVV TOMs Informationssicherheit**, Kapitel 6.3), ein vom *Auftraggeber* bereitgestelltes PAM-System nutzen, um jegliche administrative Tätigkeiten auf den Systemen des *Auftraggebers* zu protokollieren.

Der Aufruf des PAM-Systems erfolgt von Endgeräten des *Auftragnehmers*, die Anmeldung erfolgt mit einem Active Directory Account des *Auftraggebers*. Zur Vereinfachung der Administration kann der *Auftragnehmer* Sprungserver (Jump Server) provisionieren und betreiben. Die Konzepte für eine Sprungserver Lösung müssen mit dem *Auftraggeber* abgestimmt werden.

Im Falle eines Desasters oder Ausfalls des PAM-Systems muss der *Auftragnehmer* alternative Zugangswege für die Fehlerbehebung bereitstellen.

9 Anforderungen an die Connectivity & Netzwerkbasisdienste

9.1 Einleitung

Die Übersicht wird bei der Aufforderung zum indikativen Angebot zur Verfügung gestellt.

Abbildung 5: Physikalische Leitungen für Transition & Hybridbetrieb

Im Zuge der Transition werden die Bestandsservices und notwendigen Daten des *Auftraggebers* von einem Rechenzentrum der T-Systems in bis zu drei RZ- bzw. Cloud-Standorte migriert. Um den Datenverkehr zwischen den verschiedenen Dienstleistern zu ermöglichen, wird der *Auftraggeber* dedizierte Leitungen (hier Lila dargestellt) von den bestehenden Datacentern zu den neuen Standorten und das Routing bereitstellen. Diese Leitungen werden sowohl für die Datenmigration als auch für den notwendigen Hybridbetrieb während der Transition genutzt. Des Weiteren betreibt der *Auftraggeber* ein MPLS-Netz zur Standortvernetzung, welches über das Cluster Workplace die Verbindung zu den weiteren Ressourcen des Auftraggebers bereitstellt.

Während der Transition werden die neuen Standorte mittels SD-WAN Overlay-Technologie miteinander gekoppelt. Die dafür benötigten Devices und Leitungen (rote Verbindungen) stellt ein weiterer Dienstleister des *Auftraggebers*. Die Standorte können sowohl über die dedizierten Leitungen, als auch den vom jeweiligen Clusterprovider bereitgestellten Internetaccess (gelb) miteinander kommunizieren.

Der Datenverkehr zwischen den Clustern wird nach Abschluss der Transition ausschließlich über das SD-WAN geleitet, so dass der *Auftraggeber* vollständige Transparenz über die Kommunikationswege und die Möglichkeit zur Steuerung des Datenverkehrs erhält. Hierfür wird der verschlüsselte Verkehr an der Firewall des *Auftraggebers* aufgebrochen, außerdem ist dies die zentrale Stelle für Verbindungssteuerung mittels ACLs. Traffic zwischen den Clustern soll durch den jeweiligen *Auftragnehmer* explizit erlaubt sein, was den Koordinationsaufwand bei neuen Verkehrsbeziehungen vereinfachen soll. Netzwerkbasisdienste wie z.B. DNS, DHCP oder NTP werden durch den *Auftraggeber* in jedem Cluster beigestellt.

9.2 Housing von Hardware (Dedicated)

Die folgende Anforderung gilt ausschließlich für das Betriebsmodell Dedicated.

Der *Auftragnehmer* stellt dem *Auftraggeber* und Service Providern des *Auftraggebers* eine Möglichkeit bereit, dedizierte Hardware in das Betriebsumfeld des *Auftragnehmers* zu platzieren. Außerdem ermöglicht der *Auftragnehmer* dem WAN- Anbieter des *Auftraggebers* die Installation von Netz- Abschlussgeräten für dedizierte Leitungen in geeigneten Räumlichkeiten.

Diese werden zur Anbindung von weiteren Rechenzentrumsstandorten und genutzten Cloudservices des *Auftraggebers* sowie für die Transitions- und Hybridleitungen benötigt.

9.3 Hosting von Appliances

Sollten virtuelle Appliances benötigt werden, muss der *Auftragnehmer* Compute- und Storageressourcen zur Erfüllung des Einsatzzweckes zur Verfügung stellen. Diese Ressourcen werden auf Wunsch des *Auftraggebers* auch ohne Betriebssystem zur Verfügung gestellt.

9.4 Installation von Agent Software

Der *Auftragnehmer* unterstützt den *Auftraggeber* bei der automatisierten Installation von Agent Software auf den für den *Auftraggeber* betriebenen Komponenten. Diese Agenten dienen zur Anreicherung von Security, Monitoring & Management Systemen.

9.5 DNS, DHCP, IPAM, NTP

Der *Auftraggeber* stellt einen DNS Service zur Verfügung, der für alle Systeme des *Auftragnehmers* genutzt werden muss. Das DNS System kann für die Auflösung externer DNS Einträge auf DNS Server des *Auftragnehmers* zurückgreifen. Der *Auftragnehmer* muss die verwendeten, privaten IP Adressräume vorab mit dem *Auftraggeber* abstimmen. DHCP Services werden bei Bedarf exklusiv durch das DDI-System des *Auftraggebers* bereitgestellt. Außerdem wird der NTP Service durch den *Auftraggeber* auf diesem System betrieben.

9.6 Public Key Infrastructure (PKI)

Alle vom *Auftragnehmer* bereitgestellten Systeme müssen der Root Certificate Authority des *Auftraggebers* vertrauen. Zertifikate für diese Systeme werden nur durch die PKI des *Auftraggebers* erstellt. Hierfür wird auch ein geeignetes Verfahren zur Prüfung des Gültigkeitsstatus durch den *Auftragnehmer* implementiert werden, welches die Systeme des *Auftragnehmers* nutzen.

9.7 Software Defined Network

Der *Auftragnehmer* stellt sicher, dass Systeme logisch segmentiert werden können. Der Service muss sowohl skalierbar und hochverfügbar sein, beispielsweise über ein Software Defined Network.

9.8 Firewall

Der *Auftragnehmer* stellt einen hochverfügbaren Firewallservice bereit. Die Firewall ermöglicht die Segmentierung der angebotenen Services auf Netzwerkebene, dient bei Netzübergängen innerhalb des Datacenters stets als Gateway und unterstützt sowohl Applikationserkennung als auch die die Steuerung der Zugriffskontrolle anhand von Benutzer IDs. Die Firewall soll zu Analysezwecken ein Logforwarding auf Logserver des Auftraggebers durchführen. Die weiteren Anforderungen sind in Kapitel 9 Intrusion Detection- / Prevention System (IDS, IPS) beschrieben.

9.9 Load Balancer

Der *Auftragnehmer* stellt eine hochverfügbare Lösung bereit, um interne Traffic-Verteilung und Load Balancing zu ermöglichen.

9.10 Internet Access

Der *Auftragnehmer* stellt einen redundanten Internet Breakout bereit. Um auf kurzfristig steigende Anforderungen reagieren zu können, muss die Bandbreite skalierbar sein.

Der gesamte Datenverkehr wird von einem State-of-the-art Firewallcluster, bereitgestellt durch den *Auftraggeber*, analysiert und mit Hilfe eines Intrusion-Prevention-System gefiltert. Der Internet Breakout muss über ein Tier 1-Peering in Deutschland bereitgestellt werden.

9.11 Anschluss ans SD-WAN

Der *Auftragnehmer* stellt die Anbindung an das Internet und das lokale Netz sowie die Anbindung von durch den *Auftraggeber* bereitgestellten Leitungen zu weiteren Rechenzentrumsstandorten (inkl. Bestandsrechenzentrum) und Cloudservices des *Auftraggebers* sicher.

Sämtlicher Traffic zwischen den Datacentern des *Auftraggebers*, so wie ins Internet, wird über die vom Auftraggeber betriebenen SD WAN Firewall geleitet.

9.12 Anbindungen an Fabric-Provider

Die angebotenen Rechenzentrumsflächen- und Services sind an mindestens 2 WAN- Fabric-Provider angebunden, um Bandbreitenerhöhung zwischen den Standorten und in die Public Cloud der großen Hyperscaler (AWS, Azure, GCP) innerhalb von 24 Stunden zu ermöglichen.