GRASS-MERKUR
Leitlinie
Cloud Services Sicherheit

Versionierung	
Version:	v1.0.0
Stand:	20190712
Autor:	Dr. Oliver Kunert
Verteilerinformationen	
Vertraulichkeit:	offen
Verteiler:	GRASS MERKUR
Info:	GRASS-MERKUR, Kunden und Interessenten
Dokumentenstatus	
Status:	Freigabe

1 Abstrakt

Dieses Dokument soll Kunden und Interessenten an Cloud-Services der GRASS-MERUR über die grundlegenden Sicherheitseigenschaften, Verfahrensweisen, Prozesse und technischen Umsetzungen bei den Cloud-Services der GRASS-MERKUR informieren. Die in diesem Dokument getroffenen Aussagen und Darstellungen ergänzen das ISMS (Informations-Sicherheits-Management-System) der GRASS-MERKUR nach ISO/IEC 27001:2013 um die Cloud-Service-bezogenen Sicherheitselemente (Controls) in Referenz auf die Norm ISO/IEC 27017: 2015.

Inhaltsverzeichnis

2 Einleitung

Dieses Dokument ist an Kunden und Interessenten der Cloud-Services der GRASS-MERKUR GmbH & Co. KG gerichtet. Es beschreibt in Konformität mit dem internationalen Standard ISO/IEC 27017:2015 die Ausgestaltung der sicherheitsbezogenen Rahmenbedingungen, Prozesse, Vorgehensweisen, Verantwortlichkeiten bei der Bereitstellung der GRASS-MERKUR-Cloud-Service. Das Dokument ist auch an Kunden gerichtet, die sich ein Verständnis über diese Cloud-Services und deren sicherheitsbezogenen Eigenschaften verschaffen wollen.

GRASS-MERKUR bietet folgende Cloud-Service-Gruppen mit den jeweils darin eingeordneten Services an:

- Compute-Leistungen
- Speicherleistungen
- Datensicherungsleistungen

3 Technische und organisatorischer Grundlagen

Es existieren verschiedene Modelle der Bereitstellung von Cloud-Services. Diese grenzen sich mindestens durch folgende Eigenschaften von anderen IT-Services ab:

- Ressourcen-Pooling auf virtualisierter Infrastruktur
- Mandantentrennung
- Kundenzugriff über Netzwerke aus räumlicher Distanz
- Variabilität und Elastizität der Infrastruktur
- Verbrauchsbezogene Abrechnung

Diese besonderen Eigenschaften der Cloud-Services erfordern zugleich eine besondere Sicht auf den Umgang mit personenbezogenen Daten. Dafür hat GRASS-MERKUR eine zweite hier mitgeltende Leitlinie erstellt. (Leitlinie Cloud-Datenschutz)

3.1 Modellbeschreibung der Cloud-Services

GRASS-MERKUR legt in Bezug auf seine Cloud-Services folgendes Architektur-Modell zugrunde. Zur Darstellung werden Sichten auf die Cloud der GRASS-MERKUR verwendet. Im Modell gelten zwei Sichten, die als

a) ***die*** Cloud und

b) ***in der*** Cloud

bezeichnet werden sollen.

Die Cloud umfasst die Leistungen, die von GRASS-MERKUR erbracht werden. Dazu zählen:

- Betrieb des Rechenzentrums
- Betrieb der Cloud-Infrastruktur (physische Server, Appliances, Ablaufumgebungen (Hypervisors), Speichersysteme, Netzwerk, Management-Systeme) als Kernelement der Cloud-Services
- Betrieb der Sicherheitsinfrastruktur

- Betrieb der Datensicherungs-Infrastruktur
- Betrieb der Kundenschnittstelle für die Zugriffsverwaltung zur GRASS-MERKUR-Cloud
- Betrieb der Systeme zum Nachweis der vertraglichen Leistungserfüllung, zum Monitoring und zum Ressourcenverbrauch (Accounting)

Als ***in der*** Cloud werden folgende Objekte und Verwaltungsaktivitäten im Zuständigkeitsbereich der Kunden angesehen:

- Kundenapplikationen und Middleware
- Kundengastsysteme
- Kundendaten
- Konfiguration der Zugriffsberechtigungen auf Kundensysteme und Anwendungen durch den Kunden
- Datenverschlüsselung und Datenentschlüsselung, sowie das Schlüsselmanagement
- In die Verantwortung des Kunden fallen auch kundeneigene Client-Systeme, die sich mit der GRASS-MERKUR-Cloud verbinden.

Abzugrenzen von den Cloud-Services ist die netztechnische Verbindung zwischen Kunden und deren Systemen/Endgeräten und den Cloud-Services der GRASS-MERKUR. Dies bedarf fallweise je Kunde der gesonderten Betrachtung.

3.2 Verantwortlichkeitsverteilung

Entsprechend dem dargestellten Modell kommen systembedingt auf Kunden und GRASS-MERKUR geteilte Verantwortlichkeiten zu. IT-Infrastruktur aus der GRASS-MERKUR-Cloud zu nutzen bedeutet, dass sowohl dem Kunden als auch GRASS-MERKUR verschiedene wichtige nachfolgend beschriebene Rollen und Aufgaben bei Nutzung, Betrieb und dem IT-Sicherheitsmanagement in ihrem jeweiligen Verantwortungsbereich zukommen.

GRASS-MERKUR betreibt, verwaltet und überwacht die Komponenten von der Schicht des Host-Betriebssystems und der Virtualisierungsebene bis hin zum physischen Schutz der Einrichtungen, der technischen Gebäudeausrüstungen und des Rechenzentrums-Gebäudes selbst, in dem die Cloud-Services von GRASS-MERKUR betrieben werden. GRASS-MERKUR kennt jedoch nicht die Daten in den von Kunden genutzten Cloud-Services, die Konfigurationen der Kundensysteme und deren Zustand in der Cloud. GRASS-MERKUR verfügt in der Regel nicht über die Credentials zum Zugriff auf die von Kunden genutzten Cloud-Services. GRASS-MERKUR nimmt auf Informationen von Kunden auch keinen Einfluss, außer dies ist in einem Servicevertrag ausdrücklich geregelt.

Der Kunde ist verantwortlich für die Verwaltung der Gast-Betriebssysteme (einschließlich Updates und Security Patches für das Gast-Betriebssystem), der Datenbanken, der Anwendungssoftware und ganz besonders der Daten in den Systemen, auch die ggf. gewollte oder verlangte Verschlüsselung der Inhalte in der Cloud. Der Kunde erhält von GRASS-MERKUR eine Zugangsberechtigung zur Verwaltungsumgebung der GRASS-MERKUR-Cloud. Über diesen Zugang verwaltet der Kunde nach seinem Ermessen die Services und Systeme, die der Kunde in der GRASS-MERKUR-Cloud nutzt. Der Kunde kann sich durch GRASS-MERKUR weitere nicht privilegierte Benutzerkonten anlegen lassen.

Der Kunde verbindet sich von seinen Systemen außerhalb der Cloud entweder über eine direkte Leitung oder über ein VPN und das Internet. GRASS-MERKUR stellt dazu mit gängigen auf dem Stand der Technik

befindlichen Verfahren und Protokollen nutzbare Zugangspunkte zur Cloud bereit. GRASS-MERKUR unterstützt Kunden dabei, geeignete Lösungen einem anforderungsgerechten Sicherheitsniveau entsprechende Verbindungen zur Cloud zu finden und einzurichten.

Beim Betrieb und der Nutzung der Cloud-Services entstehen prinzipbedingt personenbezogene Daten, die in folgende Kategorien fallen: Konfigurationseinstellungen, Logging-Informationen und Nutzungs- bzw. Verbrauchsdaten. Diese Daten fallen in den Verantwortungsbereich der GRASS-MERKUR. Sie werden benötigt zum Nachweis vertraglich zugesicherter Leistungen, zur Fakturierung der Services gegenüber Kunden, zur Leistungssteuerung und Optimierung der Cloud-Services sowie ggf. zur Störungs- und Problemanalyse.

3.3 Steuerung von Risiken bei Cloud-Services

GRASS-MERKUR betreibt ein zertifiziertes Informations-Sicherheitsmanagement-System nach ISO 27001:2013. Die Zertifizierung gilt für die Infrastruktur, das Rechenzentrum und die Services von GRASS-MERKUR. Essentieller Teil des Management-Systems (ISMS) ist die Beherrschung von Risiken im Zuge der Entwicklung und während des Betriebs der GRASS-MERKUR-Services. Das langjährig bestehende ISMS ist auf die Cloud-Services ausgedehnt worden. Infolgedessen sind die Sicherheitseinrichtungen erweitert und um spezifische organisatorische und technische Maßnahmen ergänzt worden. Diese werden in Kapitel 4 beschrieben.

4 Sicherheitsbezogene Elemente der Cloud-Services

4.1 Informations-Sicherheits-Management-System (ISMS)

GRASS-MERKUR betreibt ein extern auditiertes und zertifiziertes ISMS nach dem Standard ISO/IEC 27001:2013, das auch die Cloud-Services einschließt. Im Rahmen dessen gelten abgeleitet aus den übergreifenden Sicherheitszielen die Vorgaben für die Cloud-Services. Das sind:

- das Risiko-Management,
- die Besonderheiten, die sich aus der Mandantenfähigkeit der Cloud-Infrastruktur hinsichtlich Ressourcen-Isolierung und Kundentrennung ergeben
- die Besonderheiten der Zugriffsteuerung, Authentisierung und der Verschlüsselung
- Bidirektionale Informationsflüsse über die Kundenschnittstelle in verschiedenen Prozessen
- die Sicherheit der virtualisiert betriebenen Infrastruktur
- Schutz der Kundendaten
- Management von Sicherheitsvorfällen
- die Prozesse Änderungs-, Kapazitäts- und Notfallmanagement

4.2 Sicherheitsbezogene Rollen und Verantwortlichkeiten

Rollen auf Kundenseite

Rollenbezeichnung	Bedeutung der Rolle
Administrator	Kunden wird ein Administrations-Account zugewiesen, über den die Geschäftsbeziehung zu GRASS-MERKUR abgewickelt wird.

Rollenbezeichnung	Bedeutung der Rolle
	Dieser Account hat vollen Zugriff auf alle Kundenressourcen innerhalb der GRASS-MERKUR-Cloud. Über diesen Account können alle Cloud-Services und Kundenressourcen verwaltet werden. Der Administrations-Account ist berechtigt weitere Benutzer-Accounts anzulegen und zu verwalten. Diesen Benutzer-Accounts können eingeschränkte Rechte zugewiesen werden, so dass die regelmäßigen Tätigkeiten nicht mit dem Administrator-Account ausgeführt werden müssen. Darüber hinaus können im Auftrag des Kunden durch Cloud-Administratoren der GRASS-MERKUR auch Technische Accounts angelegt und verwaltet werden, über welche Systeme untereinander in Verbindung treten können.
Benutzer	Über den Administrator-Account können weitere Benutzer-Accounts mit abgestuften Rechten für weitere Personen mit delegierten Aufgaben des Kunden angelegt werden. Diese Benutzer-Accounts verfügen gegenüber den Administrator-Account über eingeschränkte Rechte. Die zugewiesenen Rechte sollten den Befugnissen der Personen entsprechend granular zugewiesen werden. Mit Hilfe eines Benutzer-Accounts können weitere Benutzer-Accounts angelegt werden, die jedoch über höchstens dieselben Rechte wie der anlegende Account selbst verfügen. Kunden sollten jeder Person einen eigenen Benutzer-Account zuweisen. Technische Accounts dienen der Kommunikation von Systemen untereinander. Diese Accounts werden mit den benötigten Rechten ausgestattet, um zwischen Maschinen ohne Mitwirkung von Personen zu kommunizieren. Die technischen Accounts werden gezielt mit jenen Rechten ausgestattet, die zur beabsichtigten Kommunikation notwendig sind. Benutzer-Accounts können in Gruppen gleichen Rechteumfangs zusammengefasst werden.

Rollen bei GRASS-MERKUR

Rollenbezeichnung	Bedeutung der Rolle
Cloud-Administrator	GRASS-MERKUR-Cloud-Administratoren sind mit der Einrichtung und dem Regelbetrieb der GRASS-MERKUR-Cloud-Infrastruktur und der Cloud-Services befasst. Sie besitzen allumfassende Rechte an der IT-Infrastruktur und den Systemen, die sie betreuen, nicht jedoch an den Kundensystemen und Kundendaten. Administratoren sind der höchste fachliche Eskalationspunkt bei technischen Problemen an den Services.
Cloud-Architekt	Die Cloud-Architekten der GRASS-MERKUR kennen die grundsätzliche Funktionsweise der GRASS-MERKUR-Cloud-Services. Sie beraten Kunden bei der Auswahl der für sie geeigneten Services, unterstützen bei der bedarfsgerechten Einrichtung gewählter Services, unterstützen bei der Migration von Kundensystemen und Anwendungen in die Cloud und helfen bei der Fehlersuche und Entstörung. Die Architekten entwickeln die Cloud-Services weiter. Beschäftigte der GRASS-MERKUR können sowohl als Architekten als auch in der Rolle von Administratoren tätig sein.
Service Desk (NOC)	Das Network Operation Center (NOC) ist der Konzentrationspunkt für jegliche bidirektionale Kommunikation zwischen Kunden und GRASS-MERKUR im Regelbetrieb. Mitarbeiter des NOC können aktiv Informationen an Kunden verteilen, z.B. zu geplanten Changes, und nehmen Anfragen, Störungsmeldungen, Reklamationen und Beschwerden an. Personen des NOC steuern die Cloud-Services nicht in dem Umfang und der Tiefe, wie es ein Cloud-Ad-

Rollenbezeichnung	Bedeutung der Rolle
	ministrator tut, sie verfügen jedoch über angemessene Befugnis, um im Auftrag des Kunden im Serviceumfang vereinbarte Leistungen an der Infrastruktur und den Systemen des Kunden in der Cloud auszuführen und in begrenztem Umfang Entstörungen vorzunehmen.
Kundenbetreuer	Die Rolleninhaber wirken nicht am Betrieb der Cloud-Infrastruktur mit. Für diese Rolle besteht unter Umständen die Möglichkeit der Einsichtnahme in personenbezogene Daten, insbesondere in die Kategorie der Abrechnungsdaten.
Dienstleister	Von GRASS-MERKUR beauftragte und vertraglich gebundene Dienstleister können mit einzelnen Aufgaben betraut werden. Es wird technisch und organisatorisch sichergestellt, dass für Dienstleister tätige Personen nur über den Rechteumfang verfügen, der zur Bewältigung der vereinbarten Aufgaben absolut notwendig ist.

4.3 Geographische Lokation der Datenablage

Alle IT-Systeme, welche die GRASS-MERKUR-Cloud-Services bereitstellen, befinden sich in Deutschland am Standort Hannover. Sämtliche von Kunden in die GRASS-MERKUR-Cloud eingebrachten Inhalte werden an diesem Standort abgelegt.

Kunden, die zusätzlich dazu eine räumlich entfernte Ablage Ihrer Inhalte wünschen (Spiegelung, Duplikation), können diesen Service auf Nachfrage erhalten. Der Ablageort der gespiegelten Inhalte ist dann ebenfalls in der Bundesrepublik Deutschland.

4.4 Aus- und Fortbildung der GRASS-MERKUR-Mitarbeiter

Alle mit den GRASS-MERKUR-Cloud-Services betrauten Mitarbeiter werden regelmäßig zu allen Teilen des Informations-Sicherheits-Management-Systems geschult und weitergebildet. Mit Fortbildungsmaßnahmen und dem Ermöglichen des Zugangs zu neuesten Informationen zur IT-Sicherheit, Datenschutz, Sicherheitsvorfällen und Lagebewertungen hält GRASS-MERKUR das Wissen der Beschäftigten auf dem aktuellen Stand und schult seine Mitarbeiter zu den einschlägigen gesetzlichen Regelungen. Darüber hinaus finden aus aktuellen Anlässen heraus gezielt Informationskampagnen und Diskussionen unter Leitung des IT-Sicherheitsbeauftragten statt. GRASS-MERKUR hat seine Mitarbeiter auf den besonderen Schutz der Kundeninhalte in der Cloud und den im Zusammenhang mit der Nutzung der Cloud durch Kunden entstehenden Daten (Logfiles, Verbrauchsdaten) sensibilisiert und verpflichtet. Ferner verlangt GRASS-MERKUR von all seinen Dienstleistern denselben verantwortungsvollen Umgang damit und in diesem Bewusstsein ausgeführte Handlungen.

4.5 Informationsklassifikation und Kennzeichnung

Kunden können ihre in der GRASS-MERKUR-Cloud genutzten Ressourcen nach eigenem Ermessen bezeichnen und mit zusätzlichen Markierungen versehen, um die Ressourcen z.B. zu klassifizieren, einzuteilen und nach einer eigenen Systematik strukturiert zuzuordnen. Die Bezeichnungsmöglichkeiten und ergänzenden Attribute können im Rahmen der Erstellung und Verwaltung der Ressourcen an der Ressource selbst wahrgenommen werden.

4.6 Sicherheit des Rechenzentrums und physische Sicherheit

GRASS-MERKUR betreibt in Hannover ein Rechenzentrum, in dem die Infrastruktur der GRASS-MERKUR-Cloud-Services betrieben wird. Das Rechenzentrumsgebäude ist von außen nicht als solches erkennbar. Die genaue Lage des Rechenzentrums ist weder ersichtlich noch zugänglich. Die Außenanlage des Rechenzentrums ist tagsüber nur im öffentlichen Bereich (Besucherparkplatz) zugänglich.

Perimeterschutz

Das gesamte Grundstück ist mit einem hohen Gitterzaun umgeben. Das Areal ist mit einem Rolltor und einer Schrankenanlage an der Zufahrt zum nicht öffentlichen Parkplatzbereich ausgestattet, um hier eine ordnende und trennende Wirkung (öffentlicher/nicht öffentlicher Bereich) zu erreichen. Der Zutritt zum Gebäude ist über ein Zutrittskontrollsystem geregelt. Das Gebäude ist ohne Publikumsverkehr und von außen verschlossen. Weitere Perimeterschutzmaßnahmen sind eine Infrarot-Vorfeldüberwachung mit Alarmierung im Detektionsfall sowie die umfassende Überwachung aller Außenbereiche durch Kamerasysteme.

Zusätzlich überwachen Bewegungsmelder, Alarmanlagen und Videoüberwachung den Zutritt. Im Detektionsfall erfolgt gemäß definierter Kommunikationskette eine Alarmierung verschiedener Stellen (Polizei, Feuerwehr, Sicherheitsdienst, weitere definierte Mitarbeiter).

Zutrittsschutz

Der Zutritt zum Gebäude und den RZ-Flächen ist nur mit RFID-Transponder (Token und zugehöriger PIN) möglich. Alle Gebäudebereiche können nur von autorisierten Personen betreten werden, die über Zutrittsberechtigungen verfügen. Die Fenster sind nicht zu öffnen. Die Türen schließen selbsttätig.

Die Protokolle des Zutritts (Türen, Schleusen) werden gesichtet, stichprobenartig überprüft und archiviert.

Zutritt zu den Rechnerräumen

Der Zutritt zu den Rechnerräumen ist nur für die Systemverantwortlichen vorgesehen und durch Autorisierung mit Token und PIN gesichert. Der Zutritt zu allen sicherheitsrelevanten Bereichen ist nur für autorisiertes Personal möglich. Kunden (Nutzer) von Rechenzentrumsflächen können die jeweiligen Bereiche, für die sie zutrittsberechtigt sind, durch Eingabe von Token und PIN betreten. Technikräume für den Betrieb der Infrastruktur (z.B. Netzersatzanlage, Dieselgeneratoren, Klimatechnik) sind nur für eigene Haustechniker zugänglich.

Alle anderen Berechtigten sind auf entsprechende Zutrittskarten bzw. die Eingabe eines Systemcodes angewiesen. Der Zutritt ist 7/24 möglich. Für den Zutritt zum Gebäude außerhalb der Bürozeiten („unbedienter Betrieb“) sind definierte Prozesse einzuhalten.

Der Zutritt zum Rechenzentrum über Transponder und PIN wird über ein abgestuftes Berechtigungskonzept definiert, protokolliert und digital archiviert. Das Zutrittsverfahren lässt nur den Zutritt für die berechtigten Personen zu. Videokontrolleinrichtungen erfassen systematisch alle Zutrittsbereiche und wichtigen Systemkomponenten. Diese werden stichprobenartig in Hinblick auf Verdachtsmomente ausgewertet.

Büroräumlichkeiten:

Der Zutritt zu den Büroräumen ist nur möglich, nachdem eine mehrstufige Autorisierung über das Zutrittskontrollsysteme an den jeweiligen Eingängen (Gebäudetür, Etagentür) erfolgt ist (mit Zutritts-Token und PIN).

Gefahrenmeldeanlage

Die Gefahrenmeldeanlage (Brand-, Wasser- und Alarmdetektion) ist durchgängig über das GRASS-MERKUR-Monitoring realisiert. Im Detektionsfall werden automatische Alarmierungen von der Gebäudeleittechnik (GLT) ausgelöst und über unterschiedliche Meldewege an definierte Empfänger weitergeleitet (Sicherheits-

dienst, Polizei, Feuerwehr, definierte Mitarbeiter). Die technisch organisatorische Grundlage bildet ein entsprechend abgestimmtes Sicherheitskonzept. Das Gebäude verfügt über Brandvermeidungsmaßnahmen (teilw. Oxy Reduct), Argon-Löschanlagen, Rauchmelder und Feuchtigkeitssensoren.

Video-Überwachung

Es erfolgt eine Video-Überwachung von Zugängen, Maschinenräumen sowie anderer technischer Einrichtungen durch permanente, digitale Aufzeichnung aller Kameras. Die Aufzeichnungskapazität beträgt ca. 3-4 Monate (mit jeweiliger Überschreibung ältester Aufzeichnungen). Die Installation der Aufzeichnungssysteme befindet sich in den gesicherten Bereichen des Rechenzentrums. Eine Stichprobe der digitalisierten Bewegungsbilder im Rechenzentrum kann durchgeführt und mit den archivierten Daten (Zutrittskontrollprotokolle) abgeglichen werden, um eine Kontrolle über die Zutritte hinsichtlich Legitimität der stattgefundenen Handlungen zu erhalten.

Schlüsselverwaltung / Ausweisverwaltung

Es sind entsprechende Prozesse zur Transponderverwaltung implementiert, insbesondere in Bezug auf Entzug der Berechtigungen von Mitarbeitern nach Verlassen der Firma. Die vergebenen Zutrittsberechtigungen werden in regelmäßigen Abständen auf Aktualität überprüft.

Beaufsichtigung oder Begleitung von Fremdpersonen

Während der Arbeitszeiten („bedienter Betrieb“) wird die Gebäudetür nur für Besucher auf Anforderung über die Gegensprechanlage geöffnet.

Bei Zutritt von Besucher bzw. externer Dienstleister gelten die entsprechenden Schutzbestimmungen von GRASS-MERKUR (spezielle Prozessdefinitionen beim Zutritt zum Rechenzentrum: Umfang, besuchte Person, Zeitpunkt, Firmenname, Name mit Unterschrift, Besucherausweis, Begleitung eines Mitarbeiters/ Kameraüberwachung etc.). Besucher erhalten einen offen zu tragenden Besucherausweis. Besucher werden von Ihrem Gesprächspartner am Empfang abgeholt und am Ende wieder hinausbegleitet. Die Geht-Uhrzeit wird mit dem Auschecken aus dem Besuchersystem festgehalten.

Maßnahmen von Fremdpersonen (z.B. Serviceleistungen von Technikern) werden jeweils im Beisein eines GRASS-MERKUR-Mitarbeiters durchgeführt.

Besonderes Verfahren außerhalb der Geschäftszeiten

Zu Geschäftszeiten ist davon auszugehen, dass berechtigtes Bedienungspersonal sich regelmäßig in den Rechenzentrumsbereichen aufhält. Außerhalb dieser Zeiten ist der Zutritt über definierte Prozesse 7x24 sichergestellt.

Kontrollgänge

Im Rechenzentrum finden regelmäßige Kontrollgänge statt.

Umgang mit und Sicherheit von Datenträgern

Mobile Datenträger wie Bänder, Platten und Kassetten werden bei Bedarf nur in abgesperrten Schutzbereichen (Lampertz-Datenschutztresor) gelagert.

Gedruckte Aufzeichnungen sind, soweit diese mindestens als vertraulich eigestuft und so gekennzeichnet sind, ebenfalls im Safe gelagert. Der jeweilige Safe ist nur für einen definierten Personenkreis zugänglich, der Zugriff auf diese Dokumente haben muss.

Schutzzonen

Innerhalb des Rechenzentrums sind getrennte Bereiche für Carrier (DFÜ-Raum für Datenleitungen), Stromversorgung (Stromunterverteilung, Netzersatzanlage) und Racks (absperrbare Racks), bzw. bei einzelnen Kundenprojekten dedizierte Rechenzentrumsflächen (Cages oder private Rooms) aufgebaut, für die nur einen definierter Personenkreis Zutritt erhält.

Notausgänge

Die Rechenzentren besitzen Notausgänge nach Brandschutzverordnung; dabei wird sichergestellt, dass Alarm ausgelöst wird, wenn die nur von innen durchführbare Panikfunktion einer Tür betätigt wird.

4.7 Netztrennung, Netzwerkzugriff und Netzwerk-Services

Das Netz der GRASS-MERKUR-Cloud ist vom übrigen internen Netz der GRASS-MERKUR getrennt. Administratoren von GRASS-MERKUR steuern die Cloud-Infrastruktur über einen Zugangspunkt und verschlüsselte Verbindungen, die durch Firewalls nach dem gegenwärtigen Stand der Technik gesichert sind. Grundsätzlich sind die von den einzelnen Kunden in der GRASS-MERKUR-Cloud betriebenen Systeme und Datenspeicherbereiche von denen anderer Kunden getrennt und für diese gegenseitig nicht sichtbar. Dazu nutzt GRASS-MERKUR die in der Cloud-Infrastruktur vorhandenen technischen Möglichkeiten. Kunden können durch Netzkonfigurationen und Zugriffskontrolllisten an ihren Systemen darüber hinaus technische Mittel nutzen, um bei Bedarf einen noch höheren Schutz ihrer Systeme zu erzielen. GRASS-MERKUR wird Kunden bei der Einrichtung dieser Mechanismen unterstützen. Die von GRASS-MERKUR verwendete Infrastruktur ist diesbezüglich vor Ihrem Einsatz einer Risikobewertung unterzogen worden.

Sicherer Zugriffspunkt für Kunden

Der Datenverkehr von und zur GRASS-MERKUR-Cloud wird automatisch überwacht und auf Auffälligkeiten untersucht. Der Kundenzugriff erfolgt ausschließlich über sichere Protokolle oder über direkte, dedizierte Leitungen zwischen Kundenlokationen und dem GRASS-MERKUR-Rechenzentrum.

Kunden verbinden sich zur GRASS-MERKUR-Cloud grundsätzlich über verschlüsselte Verbindungen (HTTPS/TLS) oder über eine VPN-Verbindung (Virtual Private Network), die zwischen dem Kunden-Netz und den Kundensystemen in der GRASS-MERKUR Cloud geschaltet ist (Tunnel).

Netzwerkanschlüsse der GRASS-MERKUR

GRASS-MERKUR unterhält eine vollständig redundante Anbindung an das Internet über zwei verschiedene Internet Service-Provider (ISP).

4.8 Benutzer- und Zugriffsverwaltung

GRASS-MERKUR stellt für Kunden Gestaltungsspielräume an der Cloud-Verwaltungsplattform bei den Zugangsmöglichkeiten zu ihren Systemen in der Cloud zur Verfügung. Grundsätzlich wird zwischen Administratoren mit umfassenden Zugriffsrechten und Benutzern mit spezifisch eingeschränkten Berechtigungen unterschieden, siehe hierzu auch Abschnitt 3.2 . Die Aktivitäten von Administratoren und Benutzern werden protokolliert und können nachverfolgt werden. Administratoren der Cloud-Verwaltungsplattform der Kunden können (zukünftig) selbst zu Ihrem Kundenkonto gehörende Benutzeraccounts anlegen und damit regeln, welche Kunden-Benutzer welche Berechtigungen erhalten oder sich die mit entsprechenden Rechten ausgestatteten Benutzeraccounts durch GRASS-MERKUR Cloud-Administratoren per Auftrag anlegen lassen. Passworte für Konten müssen mit einem vorgegebenen Maß komplex sein und müssen regelmäßig geändert werden. Geschieht dies nicht nach einem vorgegebenen Zeitraum, werden die Konten deaktiviert. Für Benutzerzugänge kann bei GRASS-MERKUR beauftragt werden, dass sie temporär oder dauerhaft deaktiviert werden.

Benutzer-Registrierung und De-Registrierung

Die Vergabe und Zuordnung von Benutzerkennungen von Kundensystemen in der Cloud ist in der Verantwortung des Kunden oder kann bei GRASS-MERKUR angefordert werden. Kunden werden administrative Rechten an den von ihnen genutzten Cloud-Systemen eingeräumt, so dass die Kunden ihren Nutzern nach Bedarf selbstständig Zugriffsrechte zuweisen und entziehen können. Die Passwortverwaltung für Benutzer liegt in der Verantwortung der Kunden. Die Verantwortlichkeit liegt auch für die Fälle beim Kunden, wenn Passworte zu einem oder mehreren seiner Benutzerkonten ausgespäht wurden oder bekannt wurden und

Benutzerkonten bzw. Kundeninhalte dadurch eventuell kompromittiert worden sind. Ein einmal einem Benutzer zugewiesenes Konto sollte durch die Kundenorganisation nicht an einen anderen Benutzer des Kunden vergeben werden.

Administratoren von GRASS-MERKUR, die mit der Verwaltung der Cloud befasst sind, verfügen über jeweils eine eigene Benutzerkennung und dürfen administrative Tätigkeiten zum Zweck der Nachvollziehbarkeit nur unter ihrer eigenen Benutzerkennung durchzuführen.

Technische Benutzerkonten (Accounts)

Zur Steuerung der Zugriffe, die Maschinen untereinander ausführen, sollten anstelle von personenbezogenen Benutzerkonten technische Accounts angelegt und verwaltet werden. Die gestaltbaren Eigenschaften, wie z.B. der Rechteumfang, solcher Benutzerkonten, auch als Rollen bezeichnet, sind dieselben wie bei personenbezogenen Accounts. Technische Accounts können aus Gründen der Vereinfachung mehrfach verwendet werden.

Gruppen

Die Benutzersteuerung der GRASS-MERKUR-Cloud erlaubt die Erstellung und die Ausgestaltung von Gruppen mit spezifischen Rechten. Benutzerkonten und technische Konten können so in Gruppen arrangiert werden, dass Personen oder Maschinen, welche aufgrund der Rollenausübung dieselben Rechte benötigen, in eine oder mehrere Gruppen eingeordnet werden können.

4.9 Einsatz von Administrationsprogrammen mit privilegierten Rechten

Management-Dienstprogramme

Die Management Dienstprograme der GRASS-MERKUR-Cloud-Services sind graphische Werkzeuge oder Befehlszeilenclients (CLI), mit denen API (Application Programming Interface) -Aufrufe getätigt werden. Es gibt spezifische Werkzeuge für jeden Service. Durch gezielte Rechtevergabe an den Dienstprogrammen und den zugehörigen Steuerungsdateien ausschließlich an GRASS-MERKUR-Administratoren ist sichergestellt, dass die für Benutzer vorgesehenen Schnittstellen im Zugriff auf ihre CLOUD-Services nicht umgangen werden können. Außerdem muss ein Administrator sich gegenüber den Management-Werkzeugen authentifizieren. Die Netzwerkschnittstellen, über welche die GRASS-MERKUR-Administratoren zugreifen, befinden sich in einem separaten Management-Netzwerk, getrennt durch Firewalls.

Für das Management über ein Web-Interface wird immer die TLS-Schnittstelle wie HTTPS verwendet.

Die Nutzung der Schnittstelle und die darüber ausgeführten Kommandos werden überwacht und auf Anomalien hin automatisch untersucht.

4.10 Einsatz kryptographischer Mittel

Allgemeine Vorgabe: Kunden und GRASS-MERKUR sind gemeinschaftlich gehalten, sich in den einschlägigen Gesetzen und Vorgaben des jeweilig für Sie geltenden Rechtsraums kundig zu machen und diese bei der Auswahl der einzusetzenden Verschlüsselungsverfahren zu beachten.

Verschlüsselung ruhender in der Cloud abgelegter Daten in GM-OBJECTSTOR

Der Service GRASS-MERKUR OBJECTSTOR verfügt über verschiedene Sicherheits-Funktionen, um die darin abgelegten Daten zu schützen. Gegenwärtig verlangt GRASS-MERKUR von den Kunden, welche den GM-OBJECTSTOR nutzen wollen, die Daten bereits vor der Einbringung in den Cloud-Speicher selbst mit einem angemessenen Verschlüsselungsverfahren und geeigneter Schlüssellänge zu verschlüsseln und damit verschlüsselt anzuliefern. Der Schlüssel bleibt Geheimnis des Kunden. Weil GRASS-MERKUR den Schlüssel nicht kennt, ist GRASS-MERKUR nicht in der Lage, selbst eine Entschlüsselung der Inhalte des

Cloud-Speichers vorzunehmen. Sämtliche Funktionen des Schlüsselmanagements (wie Umschlüsselung oder Schlüsselverwaltung) bleiben dadurch aber allein Aufgabe des Kunden.

Verschlüsslung ruhender Daten abgelegt in GM-BLOCKSTOR

Der Service GM-BLOCKSTOR stellt Plattenbereiche (Volumes) unformatiert zur Verfügung. Diese Volumes können in einen in der Cloud betriebenen Server (GM-Cloud-Compute) eingebunden werden. Mehrere solches Volumes können zu einem Verbund zusammengefügt werden. Anschließend kann dieses Volume mit Betriebssystem-Mitteln mit meinem Dateisystem nach Wahl des Kunden formatiert werden. Währenddessen oder danach liegt es im Ermessen des Kunden, das Filesystem mit Verfahren, die das jeweilige Betriebssystem bereitstellt, zu verschlüsseln. Dies ist für GRASS-MERKUR vollständig transparent und die Verantwortung für die Verschlüsslung und die Verwaltung der Schlüssel liegen vollständig in den Händen des Kunden.

Verschlüsselung ruhender Daten in Datenbanken, betrieben in der GRASS-MERKUR-Cloud.

Sofern bei Kunden die Anforderung der verschlüsselten Ablage von Daten in Datenbanken besteht, sind zwei Alternativen möglich. Dies ist zum einen die Ablage bereits verschlüsselter Daten in den Feldern der Datenbank. Die Ver- und Entschlüsselung wird dabei durch die Applikation vorgenommen. Zum anderen können die von den Datenbank-Management-Systemen angebotenen Verschlüsselungsfunktionen genutzt werden.

Verschlüsslung von Daten auf dem Weg in und aus der Cloud (Benutzerzugriff)

Der Zugriff von Kunden als Benutzer oder Administratoren ihrer GRASS-MERKUR-Cloud-Services erfolgt in der Regel über das Internet oder über eine dediziert angemietete Leitung. In beiden Fällen, vorrangig jedoch bei der Übertragung über das Internet, ist es wichtig, die übertragenen Daten vor dem Fremdzugriff zu schützen. Dies umfasst auch den Schutz des Netzwerkverkehrs zwischen Clients und Servern sowie ggf. den Netzwerkverkehr zwischen Servern.

Ansätze für den Schutz von Daten im Transit beim Zugriff auf die GRASS-MERKUR-Cloud-Dienste sind:

- HTTPS-Datenverkehr (Webanwendungen): HTTP-Datenverkehr ist standardmäßig nicht geschützt. Der TLS-Schutz für HTTP-Datenverkehr, auch bekannt als HTTPS, ist Industriestandard und wird von Webservern und Browsern weitgehend unterstützt. HTTP-Verkehr kann nicht nur den Client-Zugriff auf Webseiten, sondern auch Web-Services (REST-basierter Zugriff) z.B. auf GM-OBJECTSTOR umfassen.
- RDP-Datenverkehr (Remotedesktopprotokoll): Benutzer, die auf Windows-Terminaldienste in der öffentlichen Cloud zugreifen, verwenden normalerweise das Microsoft-Remotedesktopprotokoll (RDP). Grundsätzlich können RDP-Verbindungen auf eine zugrunde liegende TLS-Verbindung zurückgreifen. Für einen optimalen Schutz sollte der Windows-Server, auf den zugegriffen wird, ein vertrauenswürdiges X.509-Zertifikat erhalten, um vor Identitäts-Spoofing oder Man-in-the-middle-Angriffen zu schützen. Standardmäßig verwenden Windows-RDP-Server selbstsignierte Zertifikate, die nicht vertrauenswürdig sind und daher vermieden werden sollten.
- Secure Shell (SSH)–Verkehr: SSH ist der bevorzugte Ansatz zum Herstellen von Verwaltungsverbindungen zu Linux-Servern. Kunden sollten SSH Version 2 einsetzen. SSH ist ein Protokoll, das wie SSL einen sicheren Kommunikationskanal zwischen dem Client und dem Server bereitstellt. Darüber hinaus unterstützt SSH auch das Tunneling, das Kunden zum Ausführen von Anwendungen wie X-Windows zusätzlich zu SSH verwenden sollten
- Wenn Clients oder Server auf Datenbanken in der Cloud zugreifen müssen, müssen sie möglicherweise auch das Internet durchqueren. Die meisten modernen Datenbanken unterstützen TLS-Wrapper für native Datenbankprotokolle. Für Datenbankserver, die auf GRASS-MERKUR Compute-Service-Instanzen ausgeführt werden, empfiehlt sich dieser Ansatz zum Schutz von Daten bei der Übertragung.
- Das GRASS-MERKUR-Cloud-Management-Interface verwendet TLS zwischen dem Client-Browser

und den Serviceendpunkten, um die Ausführung der Verwaltungsfunktionen zu schützen. Der Datenverkehr wird verschlüsselt, die Datenintegrität wird authentifiziert und der Client-Browser authentifiziert die Identität des Cloud-Service-Endpunkts mithilfe eines X.509-Zertifikats. Der gesamte nachfolgende HTTP-Datenverkehr ist mit TLS geschützt.

- Für den bidirektionalen Zugriff auf Daten in GM-OBJECTSTOR wird eine sichere TLS-Verbindung zwischen dem Clientbrowser und dem GM-OBJECTSTOR-Container hergestellt. Der gesamte nachfolgende Verkehr ist innerhalb dieser Verbindung geschützt. Wenn die Cloud-API direkt verwendet wird, wird eine TLS-Verbindung zwischen dem Client und dem Service-Endpunkt hergestellt, und anschließend wird der gesamte nachfolgende http-Datenverkehr innerhalb der geschützten TLS-Sitzung gekapselt.
- Schützen von Daten im Zugriff auf eine Datenbank in der GRASS-MERKUR-Cloud: Wenn Kunden eine Verbindung über das Internet zu einer Datenbank in der GRASS-MERKUR-Cloud herstellen, sollte TLS für die Verbindung eingesetzt werden. TLS bietet Peer-Authentifizierung über X.509-Serverzertifikate, Datenintegritätsauthentifizierung und Datenverschlüsselung für die Client-Server-Verbindung. TLS wird für Verbindungen zu MySQL- und Microsoft SQL-Instanzen unterstützt. Für beide Produkte stellt GRASS-MERKUR ein einzelnes selbstsigniertes Zertifikat bereit, das dem MySQL- oder Microsoft SQL-Listener zugeordnet ist. Kunden können das selbstsignierte Zertifikat herunterladen und als vertrauenswürdig festlegen. Dies ermöglicht die Peer-Identitäts-Authentifizierung und verhindert Man-in-the-Middle- oder Identity-Spoofing-Angriffe auf der Serverseite. TLS ermöglicht die native Verschlüsselung und Datenintegritätsauthentifizierung des Kommunikationskanals zwischen dem Client und dem Server.

Grundsätzlich stehen nachfolgend gelistete, durch die GRASS-MERKUR-Cloud-Infrastruktur unterstützte kryptographische Verfahren zur Verfügung:

Algorithmus	Schlüssellänge	Einsatzzweck	Funktion
AES	128, 192, 256 bits	Verschlüsselung	Verschlüsselte Datenübertragung, Verschlüsselung ruhender Daten
TDES	168 bits	Verschlüsselung	Protected data transfer
RSA	1024, 2048, 3072 bits	Authentifizierung, Schlüsselaustausch	Identification and authentication, protected data transfer
DSA	L=1024, N=160 bits	Authentifizierung, Schlüsselaustausch	Identification and authentication, protected data transfer
Serpent	128, 192, or 256 bits	Verschlüsselung	Verschlüsselung ruhender Daten
Twofish	128, 192, or 256 bit	Verschlüsselung	Verschlüsselung ruhender Daten
SHA-1	n/a	Hash Wert	Verschlüsselte Datenübertragung, Verschlüsselung ruhender Daten
SHA-2 (224, 256, 384, or 512 bits)	n/a	Hash Wert	Verschlüsselung ruhender Daten, Identifikation und Authentifizierung

4.11 Verwaltung elektronischer Schlüssel

GRASS-MERKUR betreibt innerhalb der Cloud-Infrastruktur keinen durch Kunden nutzbaren Verschlüsselungs-Service. Für sämtliche mit der Verschlüsselung von ruhenden oder übertragenen Daten im Zusammenhang stehende Funktionen sind die Kunden der GRASS-MERKUR-Cloud selbst verantwortlich. Cloud-Architekten der GRASS-MERKUR beraten die Kunden bei Bedarf zum Einsatz kryptographischer Mittel, Verfahren und Technologien. Dies umfasst auch die Beratung zur Anschaffung ggf. notwendiger direkter Datenverbindungen der Kundenliegenschaften zum GRASS-MERKUR-Rechenzentrum und zur Einrichtung von VPN-Lösungen bzw. zur Nutzung von TLS.

Schlüsselverwaltung und Rotation

GRASS-MERKUR empfiehlt Kunden für die Schlüsselverwaltung eine regelmäßige Rotation (Austausch).

4.12 Change Management

Veränderungen an technischen Anlagen, Geräten der Infrastruktur und IT-Systemen zur Informationsverarbeitung werden grundsätzlich dem Change Management unterworfen. Das Change Management klassifiziert Änderungen als Standard, Normal und Emergency. Standard Changes sind vorab freigegeben. Es existiert eine Liste der jeweils gültigen Standard Changes. Normal Changes durchlaufen das komplette Verfahren und müssen individuell genehmigt werden. Zur Umsetzung von Änderungen gehört es auch, das vorgeschriebene Test- und Freigabeverfahren zu befolgen. Bei kritischen Situationen kann es notwendig sein, im Sinne des Verfahrens eingestufte Emergency Changes zügig durchzuführen. In jedem Falle werden vor der Freigabe zur Umsetzung die Auswirkungen auf die bestehenden Produktions- und Sicherheitseinrichtungen sowie die Einhaltung der Sicherheitsziele untersucht. Ist abzusehen, dass Kunden der GRASS-MERKUR Cloud-Services von den Änderungen betroffen sein werden, bindet GRASS-MERKUR die Kunden in die Planung und die Bestimmung passender Umsetzungszeitpunkt ein. Kunden wird eine kurze technische Beschreibung der geplanten Aktivitäten übergeben. Vor dem Beginn der Umsetzung werden die Kunden informiert. Nach der Umsetzung von Changes werden die Kunden ebenfalls über den Erfolgsstatus informiert. GRASS-MERKUR stellt eine Rückschau an, um Ableitungen für zukünftige Changes und Verbesserungspotentiale zu identifizieren.

4.13 Kapazitätsmanagement (Capacity Management)

Um für kurzfristig auftretende Spitzenlasten und langfristig planbares Wachstum ausreichende Versorgungskapazität zur Verfügung zu stellen, werden Kapazitätsanforderungen der Services erfasst, Verbräuche laufend überwacht und daraus Vorausberechnungen zukünftig erwarteter Kapazitätsanforderungen angestellt. Bei diesen Vorausberechnungen werden neue Geschäfts- und Systemanforderungen und aktuelle und vorhersehbare Trends der Anforderungen der Kunden von GRASS-MERKUR und von GRASS-MERKUR selbst berücksichtigt. GRASS-MERKUR betreibt dazu innerhalb des ISMS einen Prozess Kapazitätsmanagement und pflegt einen Kapazitätsplan, der sowohl ausgewählte Größen der technischen Gebäudeausrüstung als auch Größen der IT-Systeme umfasst.

Die Nutzungsmöglichkeiten der Cloud-Services der GRASS-MERKUR können technisch beschränkt werden (Quotas). Dies geschieht nur in Abstimmung mit den Kunden und auf der Basis vertraglicher Regelungen. Diese Vorgehensweise schützt Kunden auch vor unerwartet hohen Rechnungen bei ggf. unkontrollierter Ressourcennutzung. GRASS-MERKUR kann auf Anfrage bei Annäherung an die vereinbarten Nutzungsgrenzen den Kunden darüber informieren und ggf. Kapazitäts- oder Nutzungserweiterungen für die genutzten Services der Kunden umsetzen.

4.14 Business Continuity Management

Zu den erforderlichen Grundschutzmaßnahmen zählt ein umfassendes Notfallmanagement, um den Betrieb auch nach größeren Ausfällen von IT-Systemen und technischen Anlagen aufrecht zu erhalten und diesen schnellstmöglich wiederherstellen zu können. Das GRASS-MERKUR-weite Notfallmanagement wird von der Geschäftsführung, dem Sicherheitsbeauftragten und den technischen Teams wahrgenommen. Für die einzelnen technischen Anlagen, das Gebäude und die IT-Infrastruktur der GRASS-MERKUR-Cloud sind individuelle konkrete Notfallvorsorgemaßnahmen und operative Reaktionen auf Notfälle als strukturierte Störfallanweisungen ausgearbeitet worden. Die Prozeduren ausgearbeiteter und dokumentierter Notfallmaßmaßnahmen werden einem Plan folgend regelmäßig überprüft und auf Wirksamkeit getestet. Dieser Prozess ist Bestandteil der ISMS. Die Anbindung an das Internet ist redundant ausgelegt und wird bei Bedarf automatisch geschwenkt.

4.15 Datensicherung und Rücksicherung

Datensicherungen sind auch bei Nutzung von Cloud-Services unverzichtbar. Sie erfordern gerade hierbei eine spezielle Beachtung, zugleich sind die grundsätzlichen technischen Ausprägungen prinzipiell ähnlich zur Ausgestaltung und Ausführung von Datensicherungen im eigenen Rechenzentrum der Kunden. Innerhalb der GRASS-MERKUR-Cloud bestehen folgende Alternativen:

a) Kunden implementieren und nutzen für die Cloud-Services eine eigene Backup-Lösung, z.B. durch Installation einer eigener Datensicherungssoftware auf GRASS-MERKUR-Cloud-Servern. Sie haben dabei freie Gestaltung sämtliche Rahmenbedingen (Ablageort und Typ der Datensicherung, Häufigkeit, Sicherungsumfang und Aufbewahrungsdauer) nach eigenem Ermessen. Die Cloud-Architekten der GRASS-MERKUR werden die Kunden hinsichtlich der Nutzung der Cloud-Services in diesem Fall beraten und bei der Einrichtung unterstützen.

b) Kunden nutzen die von GRASS-MERKUR durch die Cloud-Services angebotenen Datensicherungsmöglichkeiten per Snapshot. Die Konfiguration hinsichtlich Aufbewahrungsdauer und Häufigkeit von Snapshots ist auch hierbei frei gestaltbar.

Technische Ausprägung / Eigenschaft	Umsetzungsmöglichkeiten in der GRASS-MERKUR-Cloud
Umfang der Datensicherungen (einbeziehbare zu sichernde Objekte) und Gestaltungsmöglichkeiten des Sicherungsregimes	Durch Kunden frei bestimmbar
Ziel und Ablageorte von Datensicherungen	Innerhalb der GRASS-MERKUR-Cloud, bzw. des GRASS-MERKUR-Rechenzentrums
Backup-Methoden, Datenformate	Vom Kunden selbst implementierte Datensicherungslösung: durch Kunden frei gestaltbar Angebot durch GRASS-MERKUR: Snapshot
Verschlüsselungsoption	Vom Kunden selbst implementierte Datensicherungslösung: durch Kunden frei gestaltbar Angebt von GRASS-MERKUR: verschlüsselt, wenn das gesicherte Objekt auch verschlüsselt ist.
Aufbewahrungszeiten	Vom Kunden frei bestimmbar
Test- und Verifikationsmöglichkeiten	Vom Kunden selbst durchführbar

Möglichkeiten der Rücksicherung und Beschreibung der erwarteten Dauer	Von Kunden selbst durchführbar

4.16 System-Logs

Die Logging-Funktionen der Cloud-Services der GRASS-MERKUR können vielfältig eingestellt werden. Grundsätzlich besteht die Möglichkeit für Kunden die zu den Services der GRASS-MERKUR-Cloud gehörenden und in den Compute-Instanzen üblicherweise vorhandenen Logging-Funktionen zu aktivieren und auf ihre Bedürfnisse hin anzupassen. Der Zugriff auf die Log-Dateien ist den Kunden möglich. Die Aufbewahrungsdauer können die Kunden eigenständig vorgeben.

Es wird empfohlen zumindest folgende Aktivitäten zu protokollieren:

- Zugriff auf Audit Logs
- Veränderung der Systemzeit
- Konfiguration von Schnittstellen
- Änderungen an Benutzerkonten
- System-Reboots
- Änderungen an Kommunikationsverbindungen
- Datensicherungen und Rücksicherungen
- Automatische Ausführung von Jobs und Task Sequenzen
- Änderungen an Sicherheitsmechanismen
- Ausführung von privilegierten Systemkommandos

4.17 Administrator und Operator-Logs

Die Cloud-Services der GRASS-MERKUR können vielfältig eingestellt werden. Grundsätzlich besteht auch hier die Möglichkeit für Kunden, die zu den Services der GRASS-MERKUR-Cloud gehörenden und in den Compute-Instanzen üblicherweise vorhandenen Logging Fähigkeiten für Aktivitäten, die von privilegierten Benutzern ausgeführt werden, zu aktivieren und auf ihre Bedürfnisse hin anzupassen. Der Zugriff auf die Log-Dateien ist den Kunden möglich. Die Aufbewahrungsdauer können die Kunden eigenständig vorgeben.

Die Aktivitäten, die vereinbarungsgemäß GRASS-MERKUR-Mitarbeiter an den von Kunden genutzten Cloud-Services ausführen, werden standardmäßig protokolliert. Der Logging-Umfang entspricht dabei grundsätzlich den in Abschnitt 4.16 genannten Aktivitäten.

4.18 Zeitsynchronisation

Kunden der GRASS-MERKUR-Cloud-Services können die Uhren der innerhalb der Cloud betriebenen Systeme gegen selbst gewählte und als präzise erachtete Zeitserver synchronisieren. Alternativ stellt GRASS-MERKUR auf Anfrage solche Zeitserver zur Verfügung bzw. berät bei der Auswahl und Einrichtung der Zeitsynchronisation.

4.19 Interne Auditierung

Zum Zweck der Wirksamkeitsbewertung getroffener sicherheitsbildender Maßnahmen des vorgabenkonfor-

men Betriebs des Informations-Sicherheits-Management-Systems sowie zur Identifikation von Weiterentwicklungs- und Verbesserungspotentialen führt GRASS-MERKUR regelmäßig interne Auditierungen dieses Management-Systems durch.

Dies ist auch ausgerichtet auf die Überprüfung der Einhaltung von Mindestanforderungen den eigenen Reifegrad betreffend, um Prozessfehler zu identifizieren und um die Wirksamkeit der Security Controls zu überwachen. Die Auditierungen folgen einem vorgegebenen Auditplan und einem Auditkalender und werden mit einem intern vorgegebenen Auditkriterienkatalog je nach zu auditierendem Objekt durchgeführt.

Darüber hinaus sollen durch die Auditierungen Nicht-Konformitäten gegenüber der Norm ISO/IEC 27001:2013 aufgedeckt und deren Gründe identifiziert werden. In der Folge sollen daraus Ableitungen für Korrektur- und Vorbeugungsmaßnahmen vorgenommen werden. Korrekturmaßnahmen mit dem Ziel der Herstellung der Konformität werden in die Liste von Verbesserungsmaßnahmen übernommen und durch das Sicherheits-Management-System gesteuert. Gleiches gilt für Vorbeugemaßnahmen, die auf das ISMS oder einzelne Security Controls ausgerichtet sind. Durch die Übernahme in die Maßnahmen-Liste wird auch die Wirksamkeit der Maßnahmen nach Umsetzung verfolgt und bewertet. Gleichzeitig erlaubt die Auditierung auch, Maßnahmen zu identifizieren, um potentiell entstehenden Nicht-Konformitäten vorzubeugen. Solche Maßnahmen werden ebenfalls in der Liste geführt.

4.20 Umgang mit technischen Schwachstellen

Identifikation von Schwachstellen: GRASS-MERKUR verfolgt vier verschiedene Wege bei der Identifikation von Schwachstellen:

a) GRASS-MERKUR lässt sich regelmäßig aus einschlägigen Quellen wie Mailinglisten und Herstellerpublikationen oder das Bundesamt für Sicherheit in der Informationstechnik über existierende Schwachstellen, neuartige Angriffsmuster und weitere allgemein kommunizierte, ein weltweit signifikantes Maß erreichende Sicherheitsvorfälle informieren.

b) Durchführung von Schwachstellen-Scans mit einschlägigen Werkzeugen

c) Durchführung von Schwachstellen-Assessments nach einem strukturierten Vorgehen (Risikodetailanalyse)

d) In besonderen Fällen Durchführung von speziell zugeschnittenen Penetrationstests nach vorheriger Risikoabwägung der Rückwirkung auf die Cloud-Infrastruktur

Behebung von Schwachstellen:

Grundsätzlich wird die Exposition gegenüber jeder detektierten Schwachstelle bewertet. Ist die Schwachstelle relevant, werden Schritte zur Beseitigung ausgearbeitet und deren Realisierung eingeplant. Umzusetzende Maßnahmen können dabei sehr verschieden ausfallen. In der Mehrzahl sind dies Softwarepatches.

Behebung von Schwachstellen durch Patches:

GRASS-MERKUR geht dabei in Bezug auf die Cloud-Infrastruktur wie folgt vor: Ausgangspunkt ist das Vorliegen der Information über ein Sicherheitsupdate zu einer die Infrastruktur betreffenden Komponente. Der erste Schritt ist die Feststellung der Kritikalität des Updates anhand eines Schwachstellen-Rating-Systems. In der Regel werden die Schwachstellen in einer Scoring-Matrix in drei Kategorien abgebildet, z.B. Privileg Eskalation, Denial of Service und Information Disclosure. Das Verständnis der Art der Anfälligkeit und wo in der Infrastruktur diese auftritt, ermöglicht es begründete Antwortentscheidungen zu treffen.

- Privileg Eskalation beschreibt die Fähigkeit eines Benutzers, mit den Privilegien eines anderen Benutzers in einem System zu handeln, wobei entsprechende Berechtigungsprüfungen umgangen werden. Ein Gastbenutzer, der eine Operation ausführt, die es ihnen ermöglicht, unbefugte Operationen

mit den Berechtigungen eines Administrators durchzuführen, ist ein Beispiel für diese Art von Sicherheitsanfälligkeit.

- Denial of Service bezieht sich auf eine ausgebeutete Sicherheitsanfälligkeit, die zu Service- oder Systemstörungen führen kann. Dies umfasst sowohl verteilte Angriffe, um Netzwerkressourcen zu überwältigen, als auch Einzelbenutzerangriffe, die typischerweise durch Ressourcenzuweisungsfehler oder eingegebene Systemausfallfehler verursacht werden.
- Informationen-Offenlegung-Schwachstellen zeigen Informationen über ein System oder Operationen. Diese Schwachstellen reichen von der Offenlegung von Informationen über die Offenlegung von kritischen Sicherheitsdaten wie Authentifizierungsanmeldeinformationen und Passwörtern.

Testen der Patches

Updates werden unter Steuerung des Change Management Prozesses behandelt. Jedes Update wird in einem Testsystem getestet, bevor es in der Produktionsumgebung bereitgestellt wird. Testkriterien werden gründlich in Bezug auf Leistung Auswirkungen, Stabilität, Anwendung Auswirkungen und anderes mehr ausgewählt.

Bereitstellung der Patches

Sobald die Updates vollständig getestet sind, können sie in der Produktionsumgebung eingesetzt werden. Diese Bereitstellung wird mit einem Konfigurationsmanagement-Tool vollständig automatisiert. Vorab wird der Einsatzzeitpunkt, sofern dazu eine Serviceunterbrechung notwendig ist, mit den Kunden abgestimmt.

Einspielen der Patches und Erfolgsbewertung

Zum Einspielen freigegebene Patches werden zum vereinbarten Zeitpunkt oder wenn Kunden-Services nicht beeinflusst werden, durch GRASS-MERKUR geplant in die Produktionsumgebung eingespielt. Anschließend wird das erfolgreiche Einspielen überprüft.

4.21 Sicherheit bei Entwicklung und Einführung von Systemen und Anlagen

Der Gesamte Lebenszyklus von Systemen und Anlagen ist unter der Kontrolle des ISMS. Der Anteil, der die Phasen Anforderungsanalyse, Auswahl, Anschaffung oder Konzeption, Entwicklung, Test und Freigabe umfasst, wird mit der nachstehenden Prinzipienliste verbindlich vorgegeben. Die Sicherheitsaspekte, welche sich aus den Grundwerten Vertraulichkeit, Integrität und Verfügbarkeit ergeben, werden umfassend berücksichtigt, um dem Paradigma „Security by Design“ zu folgen, bzw. frühzeitig in der Entwicklung von Systemen und Anlagen so berücksichtigt, dass spätere, teure Nachrüstungen vermieden werden.

Die Vorgehensweise zur projektbegleitenden (unabhängig ob Anschaffungs- oder Entwicklungsprojekt) Steuerung der IT-Sicherheitsbelange ist schrittweise und wie folgt geregelt:

1. **Sicherheitscheckliste:** Der Projektleiter füllt zusammen mit dem IT-Sicherheitsbeauftragten oder einer von ihm benannten Person **die Sicherheitscheckliste** aus. Werden dabei eine oder mehrere Fragen mit „ja“ beantwortet, ist eine Schutzbedarfsfeststellung auszuführen. Falls alle Fragen der Checkliste mit „nein“ beantwortet werden, spielen Sicherheitsaspekte in dem Projekt nur eine geringe Rolle bzw. die Auswirkungen von Risiken in dem Zusammenhang werden per se akzeptiert.
2. **Schutzbedarfsfeststellung und Geschäftsschadenanalyse:** Der Projektleiter führt zusammen mit dem IT-Sicherheitsbeauftragten oder einer von ihm benannten Person die Schutzbedarfsfeststellung aus. Dabei werden die Informationswerte identifiziert und die Auswirkungen bei Verletzung der Schutzwerte (Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität) bewertet (Geschäftsschadensanalyse). In Abhängigkeit vom Ergebnis der Analyse wird anschließend vom IT-Sicherheitsbe-

auftragten der Anforderungskatalog zusammengestellt, welcher vom betrachteten System/der Anlage (unabhängig ob Anschaffung oder Entwicklung) erfüllt werden müssen. Dazu wird das **Formular Sicherheitsanforderungen** verwendet.

3. Die Projektleitung beantwortet im Formular Sicherheitsanforderungen kurz, dass, bzw. wie die Anforderungen durch das System / die Anlage erfüllt werden.

Prüfung der Anforderungserfüllung. Der IT-Sicherheitsbeauftragte prüft, ob die von der Projektleitung zum System getroffenen Aussagen dem geforderten Schutzbedarfsniveau entsprechen. Falls keine Beanstandungen sind, kann das Projekt gestartet/fortgeführt werden. Bei Beanstandungen wird die Projektleitung aufgefordert, die Erfüllung der Anforderungen nachzuarbeiten, bis alle Beanstandungen ausgeräumt sind. Sollten Anforderungen systembedingt nicht erfüllbar sein, ist die entsprechende Sicherheitsanforderung an die Security Management Task Force (SMTF) heranzutragen und eine Ausnahmegenehmigung zu erwirken. Um Projekte nicht unnötig zu verzögern, kann die Ausnahmegenehmigung auch spontan durch Entscheidung der Geschäftsführung oder des IT-Sicherheitsbeauftragten erfolgen. Dies ist im Formular Sicherheitsanforderungen zu der entsprechenden Anforderung zu dokumentieren.

Audit nach Umsetzung:

IT-Sicherheitsbeauftragten oder einer von ihm benannten Person kann nach Umsetzung des Projektes und vor Inbetriebsetzung die Überprüfung einzelner oder aller Sicherheitsanforderungen vornehmen. Dabei festgestellte Abweichungen in der Erfüllung von Anforderungen gegenüber den in Phase 3 getroffenen Angaben/Zusagen sollen begründet werden, ggf. anschließend korrigiert bzw. wiederum durch Erwirkung von Ausnahmeregelungen, wie in Phase 4 beschrieben, akzeptiert werden.

Fachliche und funktionale Abnahme

Freigaben über Änderungen an Systemen und Anlagen werden erst erteilt, nachdem eine funktionale Abnahme erfolgt ist und bei dieser Abnahme keine betriebsverhindernden Mängel, insbesondere die Sicherheit einschränkenden Mängel aufgetreten sind. Die funktionale Abnahme erfolgt auf der Basis von protokollierten Tests.

Die funktionale Abnahme soll vor allem nachweisen, dass die in den Konzepten erarbeiteten Funktionen und Abläufe erbracht werden und abgearbeitet werden können. Sollte sich im Verlaufe der Abnahme noch der Bedarf für Änderungen ergeben, dann sollten diese Änderungen so formuliert werden, dass die Hinweise im Abnahmeprotokoll als Spezifikation für die Umsetzung dieser Änderungen dienen können.

Neue IT-Systeme und Anlagen, Updates und neue Versionen von Software sind vor ihrer Übernahme in die Produktionsumgebung dem formellen Test- und Freigabeverfahren zu unterziehen. Für die Abnahme müssen Kriterien festgelegt werden, die mindestens die folgenden Aspekte beinhalten:

- Anforderungen an Leistungs- und Rechnerkapazität
- Fehlerbehebungs- und Wiederanlaufverfahren sowie Notfallpläne
- Vorbereitung und Tests von routinemäßigen Betriebsverfahren nach definierten Normen
- Maßnahmen für die Aufrechterhaltung des Geschäftsbetriebs
- Nachweis, dass die Installation des neuen Systems existierende Systeme nicht beeinträchtigt, insbesondere zu Spitzenzeiten der Verarbeitung wie dem Monatsende
- Nachweis, dass die Gesamtsicherheit der Informationsverarbeitung von GRASS-MERKUR durch das neue System maximal in dem Maße beeinträchtigt wird, wie es in dem vorliegenden Dokument eingeräumt wird.

4.22 Steuerung von Dienstleistern

Werden Dienstleistungen von Dritten bezogen oder wird die Leistungserstellung der GRASS-MERKUR

durch Dritte unterstützt, sind damit besondere Risiken verbunden, welche mittels folgender Regelungen beherrschbar gemacht werden.

Die Aktivitäten im Management der Beziehungen zu Dienstleistern gliedern sich wie folgt:

a) Vorabtätigkeiten und Dienstleistereinbeziehung

b) Vertragsgestaltung unter Berücksichtigung von Sicherheitsanforderungen

c) Steuerung des Leitungsbezugs im Regelbetrieb

d) Rückübertagung oder Verlagerung von Leistungen zu einem anderen Dienstleister

Vorabtätigkeiten und Dienstleistereinbeziehung

- Jeder Dienstleister, der im Rahmen der Erfüllung seiner ihm übertragenen Aufgaben Zugriff auf Systeme oder Daten der GRASS-MERUR hat, soll zusammen mit der Beschreibung der Informationen und der Art der Zugriffsmöglichkeiten identifiziert werden.
- Das Potential für Beeinträchtigungen der IT-Sicherheit soll im Rahmen der Risikoidentifikation erkannt und bewertet werden.
- Verträge mit Dienstleistern sollen anforderungsgerecht ausgestaltet werden. Näheres dazu wird in einem folgenden Abschnitt erläutert.
- Die Sicherheitsanforderungen, welche ein Dienstleister zu erfüllen hat, sollen spezifiziert werden.
- Die Schnittstellen und Prozesse zwischen GRASS-MERKUR und jedem Dienstleister sollen abgestimmt werden. Dabei sind mindestens die Prozesse Incident Management, Change Management und Continuity Management einzubeziehen.
- Dienstleister sollen darstellen, wie auf ihrer Seite für IT-Sicherheitsbewusstsein gesorgt und wie dies langfristig aufrechterhalten wird.

Vertragsgestaltung unter Berücksichtigung von Sicherheitsanforderungen

Folgende Gesichtsunkte werden bei der Vertragsgestaltung mit Dienstleistern berücksichtigt:

- Regelung des Rechtsraumes, der Vertragssprache und des Gerichtsstands
- Prüfung der Verträglichkeit der AGB des Dienstleisters mit den eigenen Rechtsvorgaben
- Beschreibung der Maßnahmen zur Gewährleistung der Informationssicherheit
- Verpflichtungen beider Vertragsparteien über die Einhaltung von getroffen Regelungen zu Sicherheit von Objekten, Systemen, Anlagen und IT-Komponenten, die Ausführung von Aktivitäten und die Regelungen zur Einbeziehung von Sub-Unternehmern und Berücksichtigung des Leistungserbringungsorts
- Benennung sämtlicher Sub-Unternehmer zusammen mit deren Teilleistungen
- Mitteilungspflichten, Prozessbeteiligungen, Verantwortlichkeiten und Eskalationsebenen
- Festlegung von Einflussnahme- und Durchgriffsmöglichkeiten der GRASS-MERKUR auf das Sicherheitsniveau und die technische und operative Ausgestaltung
- Informationsplicht des Dienstleisters über Datenschutzverletzungen und IT-Sicherheitsvorfälle in dessen Verantwortungsbereich
- Festlegung der Prüfrechte von GRASS-MERKUR
- Regelungen für die Vertragsbeendigung und die Rückführung bzw. Übertragung sämtlicher Daten sowie das endgültige, unwiederbringliche Löschen von Daten

Steuerung der Informationssicherheit beim laufenden Bezug von Leistungen von Dienstleistern

Die Informationssicherheit muss auch im laufenden Betrieb gewährleistet werden. Dazu ist auch für die bezogenen Leistungen ein Betriebshandbuch zu erstellen, in dem die Sicherheitsaspekte berücksichtigt werden. Dabei unterscheiden sich die Einzelaufgaben generell nicht von denen, die zu planen und durchzuführen sind, wenn die IT-Systeme und Anwendungen noch in Eigenregie betrieben würden.

Die Verantwortung für die Steuerung der Dienstleister ist einer Person oder einem Team zu übertragen. Auf der Seite jedes Dienstleisters sollte ebenfalls eine dedizierte Person mit der Wahrnehmung der Schnittstellenfunktion beauftragt werden.

Besonderheiten ergeben sich jedoch dadurch, dass die Aufgaben auf mehrere Parteien verteilt sind und daher zusätzliche Aufgaben (z. B. Abstimmungen und Kontrollen) anfallen. Diese sind unter anderem:

- Die Beschäftigten der GRASS-MERKUR sind in der Kommunikation mit den Dienstleistern zu unterweisen. In der Regel sind die Beschäftigten dabei mit wechselnden und unbekannten Ansprechpartnern konfrontiert. Dies birgt die Gefahr des Social Engineering (z. B. Anruf eines vermeintlichen Mitarbeiters des Sicherheitsteams des Dienstleisters).
- Dienstleister müssen die relevanten Abläufe, Applikationen und IT-Systeme der GRASS-MERKUR genau kennen lernen und dahingehend eingewiesen werden.
- Der störungsfreie Betrieb ist durch genaue Ressourcenplanung und Tests sicherzustellen.
- Anwendungen und IT-Systeme, die der Dienstleister übernehmen soll, müssen ausreichend dokumentiert sein. Die Prüfung der Dokumentation auf Vollständigkeit muss dabei ebenso bedacht werden wie das Anpassen der vorhandenen Dokumentation auf die veränderten Randbedingungen durch den Bezug der IT-Leistungen von einem Dienstleister. Die Dokumentation neuer Systeme und die Fortschreibung der Dokumentation an sich müssen dabei ebenfalls sichergestellt sein.
- Während des Leistungsbezugs muss ständig überprüft werden, ob die Verträge oder die vorgesehenen Sicherheitsmaßnahmen angepasst werden müssen.
- GRASS-MERKUR soll sich davon überzeugen, dass auf Seiten der Dienstleister ein adäquates Notfallvorsorgekonzept existiert und umgesetzt ist.
- Die geltenden Sicherheitskonzepte aller Beteiligten müssen daraufhin geprüft werden, ob sie noch aufeinander abgestimmt sind und das gewünschte Sicherheitsniveau gewährleisten. Insbesondere sollte der Dienstleister GRASS-MERKUR zeitnah über wichtige Änderungen in seinem Einflussbereich informieren.
- Mitarbeiter und Beschäftigte von Dienstleistern und Partnern sollen angehalten werden, beobachtete oder verdächtige Schwachstellen in Systemen oder Diensten zu melden.

Regelmäßige Abstimmungsrunden zu folgenden Punkten sind abzuhalten:

- Informationsaustausch zwischen den Parteien (z. B. zu Personalnachrichten, organisatorischen Regelungen, Gesetzesänderungen, geplanten Projekten, vorgesehenen Tests und Systemänderungen, die zu Beeinträchtigungen der Dienstleistungsqualität führen können).
- Identifikation von Problemen
- Gegenseitiges Feedback und das Aufspüren von Verbesserungspotentialen.
- Änderungsmanagement: Änderungswünsche (Hardware, Software, Ausweitung des Dienstleistungsportfolios, gestiegener Ressourcenbedarf etc.) sollten frühzeitig besprochen werden.
- Reaktion auf Systemausfälle (Teilausfall, Totalausfall) Wiedereinspielen von Datensicherungen
- Beherrschung von Sicherheitsvorfällen

Notfallvorsorge für bezogene Dienstleistungen

- Generell müssen Notfallvorsorgekonzepte für die Systeme bei den Dienstleistern sowie für die Schnittstellen zwischen GRASS-MERKUR und Dienstleister (z. B. Netzverbindung, Router, Telekommunikationsprovider) existieren und regelmäßig fortgeschrieben werden.
- Hierbei gelten grundsätzlich die gleichen Anforderungen und Regelungen, wie sie in dem vorliegenden Handbuch an anderer Stelle für selbst betriebene IT-Systeme und Anwendungen vorgegeben sind.
- Besonderheiten bei bezogenen Leistungen ergeben sich dadurch, dass die Notfallvorsorge zwischen den Parteien aufgeteilt werden muss. GRASS-MERKUR soll im Rahmen der Dienstleitersteuerung auch nachhalten, ob die Grundlagen für eine langfristige Geschäftsbeziehung weiterhin gegeben sind. Überraschungen durch Wegfall oder Störungen im Leistungsbezug sollen dadurch möglichst vermieden werden.
- Überwachung und Rückschau auf die Leistungserstellung der Dienstleister
- Die in diesem Abschnitt aufgeführten Aktivitäten und Regelungen sollen dazu beitragen, dass die Ausführung der zugesicherten IT-Sicherheitsanstrengungen auf Seiten der Dienstleister durch GRASS-MERKUR überwacht wird und eine Ergebniskontrolle möglich ist.
- Dazu sind im Supplier-Management Prozess folgende Ziele zu verfolgen und Aktivitäten auszuführen.
- Überwachung der Leistungen des Dienstleisters und die Einhaltung der Vertragsinhalte
- Rückschau auf die Leistungserstellung in einem festgelegten Zeitraum
- Definition von Berichtsinhalten und Berichtsperioden durch GRASS-MERKUR
- Einforderung, Annahme und Auswertung der Berichte
- Planung und Durchführung von Kontrollen beim Dienstleister
- Definition und Steuerung von Regelungen zum Umgang mit IT-Sicherheitsvorfällen, insbesondere der Kommunikation dazu zwischen Dienstleister und GRASS-MERKUR
- Feststellung von Problemen und gemeinsame Suche nach strukturellen Lösungen
- Gemeinsame Klärung bei GRASS-MERKUR wahrgenommener Leistungsstörungen
- Abstimmungen über Planungen, Kapazitätsauswertungen, Notfallbehandlungsplanungen und Veränderungen

GRASS-MERKUR muss die Gesamtkontrolle und Einsichtnahme in alle Sicherheitsaspekte behalten sowie eingebunden sein in die Schwachstellenbehandlung, das Change Management und die Behandlung von IT-Sicherheitsvorfällen. Dazu sollten regelmäßige Besprechungen zur Rückschau auf die erbrachten IT-Leistungen, zur gegenwärtigen Situation und zu Planungen etabliert und durchgeführt werden.

Umgang mit Änderungen an den Leistungen

Die Services und die Verträge mit Dienstleistern müssen dem Change Management unterzogen werden. Das Change Management muss bei den nachfolgend aufgezählten Vorgängen aktiviert werden. Es ist dabei unerheblich, von welcher Partei die Veränderungen ausgelöst werden.

- Formale Änderungen an Vertragsumfängen und Leistungsparametern
- Einführung neuer Systeme und Anwendungen
- Veränderungen an Services

- Modifikationen an IT-Systemen und Anwendungen
- Einführung, Veränderung oder Stilllegung von Steuerungsmitteln zur Einhaltung der Sicherheitsvorgaben
- Einführung neuer Technologien
- Einführung, Veränderung oder Stilllegung von Werkzeugen und Ablaufumgebungen
- Ortsveränderungen von IT-Systemen und Ortsveränderungen der Leistungserstellung
- Austausch von Sub-Dienstleistern
- Hinzunahme weiterer Dienstleister

Regeln für eine geordnete Beendigung des Dienstleisterverhältnisses

Bereits in der Phase der Vertragsgestaltung mit dem Dienstleister sollten folgende Punkte, die sich auf eine etwaige Beendigung des Vertragsverhältnisses beziehen, geregelt werden.

Wird das Dienstleistungsverhältnis beendet, müssen die betroffenen IT-Leistungen geordnet wieder zurück in die eigene Verantwortung oder auf einen anderen Dienstleister übergehen können. Dazu müssen Vorkehrungen getroffen werden, die verhindern, dass durch das Vertragsende des Dienstleistungsvertrags die IT-Serviceleistungen beeinträchtigt werden.

Der Übergang hin zu einem anderen Dienstleister ist aus Sicht von GRASS-MERKUR wie das Eingehen eines neuen Dienstleisterverhältnisses vorzunehmen. Die Regelungen, die bei erstmaliger Verlagerung von IT-Leistungen zu einem Dienstleister gelten, finden auch hier Anwendung.

Bei einer Rückverlagerung zu GRASS-MERKUR oder der Verlagerung von Serviceleistungen zu einem anderen Dienstleister sind folgende Gesichtspunkte zu beachten:

- Eigentumsrechte an Hard- und Software (Schnittstellenprogramme, Tools, Makros, Lizenzen) sind zu regeln.
- Die Weiterverwendung der vom Dienstleister eingesetzten Tools, Prozeduren, Skripte ist für den Fall der Beendigung des Dienstleistungsverhältnisses zu regeln.
- IT-Systeme, IT-Anwendungen und Arbeitsabläufe müssen durch den Dienstleister ausreichend dokumentiert sein.
- Alle notwendigen Daten müssen vom Dienstleister an GRASS-MERKUR übertragen bzw. übergeben werden.
- Es ist zu veranlassen und schriftlich bestätigen zu lassen, dass nach der erfolgreichen Verlagerung alle Datenbestände beim Dienstleister unwiederbringlich gelöscht wurden.
- Interne oder externe Mitarbeiter, die Aufgaben des Dienstleisters übernehmen werden, müssen eingewiesen und geschult werden.
- Für eine Übergangsfrist, beispielsweise drei Monate, ist zu vereinbaren, dass der bisherige Dienstleister noch zur Klärung von Fragestellungen und für Hilfeleistungen zur Verfügung steht.

4.23 Umgang mit Sicherheitsvorfällen

Alle Störungen an der GRASS-MERKUR-Infrastruktur und an IT-Services werden über den Incident-Management-Prozess abgewickelt. Sicherheitsbezogene Incidents werden innerhalb dieses Prozesses herausgehoben behandelt und einer besonderen Nachbetrachtung unterzogen. Sind von Kunden genutzte Systeme oder Services von einem Incident betroffen, werden die Kunden darüber benachrichtigt und ggf. in den weiteren Incident-Behandlungsprozess eigebunden. Nach Abschluss des Incidents werden die betroffenen

Kunden darüber benachrichtigt.

4.24 Kommunikation von Sicherheitsvorfällen

Vorfälle (Incidents), die als sicherheitskritisch eingestuft werden, sollen zwischen Kunden und GRASS-MERKUR gegenseitig bekannt sein. Dazu sind Informationen über eine Schnittstelle beiderseits auszutauschen. Für GRASS-MERKUR ist die Schnittstelle das NOC (Network Operation Center), siehe auch Kapitel 4.2 Auf Kundenseite ist ebenfalls eine Kontaktstelle zu benennen. GRASS-MERKUR wird, der Cloud-Plattform zuordenbare und als sicherheitsrelevant eingestufte Incidents unverzüglich an den/die jeweils betroffenen Kunden signalisieren, zusammen mit Informationen zum Ausmaß des Vorfalls und einem Vorschlag zu passenden Reaktionen darauf, ggf. auch mit Umgehungslösungen und sofern bekannt einer Information zur Dauer bis zur Bereinigung des Incidents. Umgekehrt sollen Kunden GRASS-MERKUR, adressiert an das NOC, ebenfalls bei Bekanntwerden solche Informationen an GRASS-MERKUR melden. GRASS-MERKUR wird die Incidents in eigenen Systemen dokumentieren und deren Status bis zur abschließenden Bereinigung verfolgen. Das schließt einen regelmäßigen Austausch zwischen Kunde(n) und GRASS-MERKUR zum Status-Update des(r) Incident(s) mit ein.

4.25 Beweissicherung bei Sicherheitsvorfällen

Eine der ersten Reaktionen bei entdeckten Sicherheitsvorfällen ist die Sicherung von Beweisen. GRASS-MERKUR wird hier im Verlauf des Incident Management Prozesses die zur Verfügung stehenden Mittel wie Logging-Informationen und andere beweiskräftige Spuren sichern und für eigene Untersuchungen sowie für potentielle Anforderungen von Ermittlungsbehörden vorhalten. Untersuchungen werden nur an Informationen ausgeführt, die in den Verantwortungsbereich von GRASS-MERKUR fallen (***die Cloud***). Sind Kundenressourcen betroffen (***in der Cloud***), werden Untersuchungen nur in Abstimmung und in Kooperation mit dem betroffenen Kunden ausgeführt.

Üblicherweise wird eine staatliche Stelle, die Zugriff auf die Daten eines Unternehmens nehmen will, ihr Auskunftsverlangen direkt an dieses Unternehmen richten, anstatt sich an GRASS-MERKUR zur Herausgabe dieser Daten zu werden. Die Europäische Union (EU) hat Gesetze erlassen, wonach die öffentlichen Strafverfolgungsbehörden und nationale Sicherheitsbehörden zum Zugriff auf Informationen ermächtigt werden. Auch ausländische Strafverfolgungsbehörden können mit den lokalen Strafverfolgungsbehörden und nationalen Sicherheitsbehörden über Hilfeersuchen kooperieren, um Zugriff auf Informationen in Deutschland zu erhalten. In der Praxis wird eine staatliche Stelle nachweisen müssen, dass es einen stichhaltigen Grund für das Zugriffsverlangen auf die Inhalte gibt, und sie wird einen Gerichtsbeschluss oder Durchsuchungsbefehl erwirken müssen. GRASS-MERKUR wird Kundeninhalte nicht offenlegen, außer dies ist erforderlich, um rechtlich bindenden Anordnungen wie einer richterlichen Anordnung nachzukommen.

GRASS-MERKUR wird jedes Ersuchen zur Herausgabe von Kundeninhalten sorgfältig prüfen und auf Konformität zu geltendem Recht verifizieren. Ist GRASS-MERKUR demnach rechtlich abgesichert gezwungen, Kundeninhalte herauszugeben, werden Kunden vor der Herausgabe über das Ersuchen informiert, und den Kunden wird damit die Möglichkeit eingeräumt, sich juristisch gegen die Herausgabe zu wehren.

4.26 Berücksichtigung anwendbarer Gesetze und Vorgaben

Das Informations-Sicherheits-Management-System (ISMS) der GRASS-MERKUR umfasst in seinen regelmäßigen Aktivitäten auch die Beobachtung der gesetzgebenden Instanzen hinsichtlich für IT-Service-Betreiber geltender Gesetze und deren Novellierungen. GRASS-MERKUR wird die eigene Betroffenheit überprüfen, sich, falls notwendig, unverzüglich darauf ausrichten und Kunden vorab über sich ändernden Rahmenbedingungen informieren. Auf Anfrage weist GRASS-MERKUR die gesetzeskonforme Auslegung der Services und deren Leistungserstellung Kunden gegenüber nach.

Cloud-Service Kunden der GRASS-MERKUR werden vor der Nutzung der Services auf die einschlägigen geltenden Gesetze hingewiesen und können bei Bedarf zu ihrer eigenen Ausrichtung dazu beraten werden. GRASS-MERKUR kann jedoch nicht alle branchenüblichen Regelungen, die für Kunden im speziellen Einzelfall gelten könnten, kennen und verweist deshalb alle Kunden darauf, hierzu eigene Recherchen anzustellen, sich ggf. juristischen Rat zu suchen und danach zusammen mit GRASS-MERKUR nach Lösungen zu suchen, die Nutzung der Cloud-Services der GRASS-MERKUR gesetzeskonform zu gestalten. Insbesondere gilt dies für den Einsatz von Verschlüsselungsverfahren.

4.27 Lizenzmanagement und Schutz geistigen Eigentums

In Bezug auf den Schutz des geistigen Eigentums und das Lizenzmanagement gelten die bereits im Kapitel 3.1 zur geteilten Verantwortlichkeit zwischen Kunden und GRASS-MERKUR dargestellten Grundsätze. Für das Lizenzmanagement bedeutet dies insbesondere, dass sich die Kunden über Lizenzierungsarten und Lizenzumfänge der von ihnen genutzten Services innerhalb der GRASS-MERKUR-Cloud selbst informieren müssen und dafür abschließend verantwortlich sind, um zu jedem Zeitpunkt rechtskonform zu agieren. GRASS-MERKUR wird für seinen Teil die Verantwortung über die Lizenzkonformität der Cloud-Infrastruktur sicherstellen. Darüber hinaus wird GRASS-MERKUR eng mit Kunden zusammenarbeiten und Kunden beraten, um die Lizenzkonformität herzustellen und zugleich den wirtschaftlichen Einsatz durch passend angewendete Lizenzmodelle zu bewirken und mögliche Synergiepotentiale auszuschöpfen.

4.28 Schutz von Dokumenten und Aufzeichnungen über die Nutzung der Cloud-Services

Über die Nutzung der Cloud-Services der GRASS-MERKUR durch Kunden werden zum Nachweis der erbrachten Leistung (als rechnungsbegründende Unterlagen), für analytische Zwecke zur zukünftigen Prävention von Fehlern, zur Problembehandlung und zur Beweissicherung Informationen gespeichert und über einen Zeitraum von mindestens fünf Jahren vorgehalten. Die anfallenden Daten werden an einem zentralen Ort, abgegrenzt von der Cloud-Infrastruktur und nur für Administratoren von GRASS-MERKUR zugreifbar abgelegt.

4.29 Zertifizierung der Informationssicherheit der Cloud-Services (und unabhängige Bewertung)

Für GRASS-MERKUR haben die drei Dimensionen der IT-Sicherheit (Verfügbarkeit, Vertraulichkeit und Integrität) immer höchste Priorität. GRASS-MERKUR erbringt Services für anspruchsvolle Kunden, die ihrerseits hohe Ansprüche erfüllen wollen oder müssen. Deshalb betreibt GRASS-MERKUR seit 2012 durchgängig ein zertifiziertes Informations-Sicherheitsmanagement-System (ISMS), das dem Standard ISO/IEC 27001 entspricht. Die Zertifizierung belegt, dass GRASS-MERKUR seine Services mit wirksamem Risiko-Management und auf hohem Sicherheitsniveau erbringt.

GRASS-MERKUR lässt sein Informations-Sicherheits-Management-System (ISMS) und seine Cloud-Services jährlich durch eine externe, unabhängige Organisation untersuchen und zertifizieren. Die zur Prüfung herangezogenen Standards sind ISO/IEC 27001:2013, ISO/IEC 27017:2015 und ISO/IEC 27018:2014. GRASS-MERKUR erbringt mit der Vorlage der Zertifikate gegenüber Kunden und Interessenten den Beweis und dokumentiert den unbedingten Willen Kunden gegenüber höchsten Ansprüchen an Sicherheit seiner IT-Services und den Datenschutz erfüllen zu wollen. Zugleich schafft GRASS-MERKUR damit Transparenz für seine Services und seine Leistungserstellung.

4.30 Rückübertragung von Kunden-Software und Kundendaten

nach Nutzungsende

Von Kunden in die GRASS-MERKUR-Cloud eingebrachte Inhalte werden nach Vertragskündigung zügig und vollständig an den Kunden zurückgegeben oder an einen anderen Dienstleister im Auftrag des Kunden weitergegeben. Die Anforderung zur Zusammenstellung der zurück- oder weiterzugebenden Ressourcen und die Durchführung dessen obliegt dem Kunden. GRASS-MERKUR stellt gängige technische Verfahren und Formate dazu bereit. Anschließend kann der Kunde seine Inhalte und von ihm genutzte Systeme in der GRASS-MERKUR-Cloud einschließlich eventuell vorhandener Datensicherungen unwiederbringlich löschen oder GRASS-MERKUR damit beauftragen. Im Zusammenhang mit der Nutzung der Cloud-Services angefallene Konfigurationsdaten, Logging-Daten und Verbrauchsdaten werden von GRASS-MERKUR nach Ablauf verpflichtender Aufbewahrungsfristen unwiederbringlich gelöscht. Zur Vernichtung der Daten und Kundeninhalte werden marktübliche und anerkannte Verfahren nach dem Stand der Technik eingesetzt, welche die Unwiederbringlichkeit sicherstellen. Dazu gehören Überschreiben, Entmagnetisierung oder physische Zerstörung von Datenträgern. GRASS-MERKUR kann damit auch nachweislich kompetente und vertrauenswürdige und vertraglich gebundene Dienstleister beauftragen.

4.31 Sicheres Löschen, Datenträgervernichtung und IT-Komponentenentsorgung

Wenn ein Kunde Inhalte in der GRASS-MERKUR-Cloud löscht, werden sie unlesbar oder unbrauchbar gemacht und die zu Grunde liegenden Speichereinheiten in der GRASS-MERKUR-Cloud, die zur Speicherung der Inhalte verwendet wurden, werden mit Methoden nach dem Stand der Technik gesäubert, bevor sie wieder vergeben und überschrieben werden. Die GRASS-MERKUR-Verfahren sehen auch sichere Stilllegungsprozesse und Vernichtungsprozesse vor, die durchgeführt werden, bevor IT-Komponenten oder Speichermedien, die zur Erbringung der GRASS-MERKUR-Services verwendet wurden, entsorgt werden. Als Teil dieser Prozesse werden Speichermedien entmagnetisiert oder gelöscht und physisch zerstört oder nach dem Stand der Technik unbrauchbar gemacht.

Die Aufbewahrung der Daten, die im Rahmen der auftragsgemäßen Leistungserfüllung anfallen, wird auf das gesetzlich und zweckgebunden erforderliche Maß begrenzt. Anschließend werden die Daten unwiederbringlich gelöscht. Auskünfte zur tatsächlichen Aufbewahrungsdauer einzelner Daten erteilt GRASS-MERKUR auf Anfrage.

4.32 Schutz der virtualisieren Umgebungen in der Cloud-Infrastruktur

Virtualisierungsumgebung

In der GRASS-MERKUR-Cloud werden Hypervisor für die Virtualisierung der Serverinstanzen (Gastsysteme) eingesetzt. Gastsysteme sind auf den Hypervisor angewiesen, um Operationen zu unterstützen, die normalerweise privilegierten Zugriff erfordern. Ein Gastbetriebssystem hat keinen direkten Zugriff auf die CPU. Eine CPU bietet vier Stufen von Privilegien: 0-3, sogenannte Ringe. Ring 0 ist am meisten privilegiert und 3 am wenigsten. Das Host-Betriebssystem wird in Ring 0 ausgeführt. Anstatt jedoch in Ring 0, wo die meisten Betriebssysteme normalerweise ausgeführt werden, läuft das Gastbetriebssystem in einem weniger privilegierten Ring 1 und Anwendungen laufen in dem am wenigsten privilegierten Ring 3. Diese explizite Virtualisierung der physischen Ressourcen führt zu einer klaren Trennung zwischen Gastsystem und Hypervisor, was eine zusätzliche Sicherheitstrennung zwischen beiden schafft.

Isolierung von virtualisierten Server-Instanzen gegeneinander

Verschiedene virtualisierte Server-Instanzen, die auf derselben physischen Maschine ausgeführt werden, werden über einen Hypervisor voneinander isoliert. Darüber hinaus befindet sich eine Trennung innerhalb der Hypervisor-Schicht zwischen der physischen Netzwerkschnittstelle und der virtuellen Schnittstelle der

Instanz. Alle Pakete müssen diese Schicht durchlaufen. Durch diese Trennung haben die Nachbarn einer Instanz keinen Zugriff mehr auf andere Instanzen und können so betrachtet werden, als befänden sie sich auf separaten physischen Hosts. Der physische Systemspeicher (RAM) wird unter Verwendung ähnlicher Mechanismen getrennt.

Kundeninstanzen haben keinen Zugriff auf Raw-Festplattengeräte, sondern diesen Instanzen werden stattdessen virtualisierte Festplatten zugewiesen. Die Datenträgervirtualisierungsschicht setzt automatisch jeden vom Kunden verwendeten Speicherblock zurück, sodass die Daten eines Kunden nie unbeabsichtigt einem anderen ausgesetzt werden. Darüber hinaus wird der den Gästen zugewiesene Speicher vom Hypervisor gesäubert (überschrieben), wenn er keiner Instanz zugewiesen ist. Der Speicher wird nicht in den Pool des für neue Zuweisungen verfügbaren freien Speichers zurückgegeben, solange die Speicher-Säuberung nicht abgeschlossen ist.

Speichervirtualisierung:

Kundendaten können in folgenden Formen und Ablageorten vorkommen:

- Objcect Speicher Inhalte
- Compute-Instanz Filesysteme
- Compute-Instanz RAM
- Block Speicher Instanzen
- Images von virtuellen Maschinen
- Datensicherungen und Snapshots

Durch die systematischen Eigenschaften der Cloud-Infrastruktur bedingt teilen sich in der Regel verschiedene Mandanten die physischen Speicherbereiche, in denen die Kundendaten abgelegt sind. Die Virtualisierungsschicht der Cloud-Infrastruktur stellt jedoch sicher, dass Kunden nur auf die organisatorisch ihnen zugeordneten Daten zugreifen können.

4.33 Härtung der virtualisierten Maschinen

Für Kunden in der GRASS-MERKUR-Cloud standardmäßig einsetzbar vorbereitete virtuelle Systeme (Images) sind gemäß den Empfehlungen der Betriebssystemhersteller in der jeweils aktuellen Fassung von GRASS-MERKUR vorab gehärtet worden. Grundsätzlich umfassen die Härtungsmaßnahmen z.B. Schließen nicht benötigter offener Ports, Stilllegung nicht benötigter Dienste oder Entfernen ganzer Softwarepakete aus dem Standardumfang, die Beschränkung der Zugriffsmöglichkeiten nur auf verschlüsselte Verbindungen, Restriktionen im Speicherzugriff, Deaktivierung/Entfernung nicht benötigter Benutzer und die Einschränkungen von Benutzerberechtigungen auf Dateien und Verzeichnisse. Grundsätzlich sind das Systemlogging und eine Basisüberwachung aktiviert und der Schutz vor Malware ist eingerichtet.

Darüber hinaus kann ein Kunde selbst weitere Härtungsmaßnahmen nach seinem Ermessen durchführen, respektive das Logging und die Systemüberwachung anpassen. Die Umsetzung weiterer Schutzmaßnahmen durch den Kunden ist ebenfalls möglich.

4.34 Sicherheit bei der Systemadministration

Kritische Operationen an den Cloud-Services

Es ist für Administratoren der Kunden zwingend notwendig, Steuerungsfunktionen an den von ihnen genutzten Cloud-Services und beteiligten Komponenten auszuführen. In dieser Hinsicht ist es wichtig, dass die Be-

fehls- und Kontrolleinrichtungen von den Administratoren der Kunden gekannt und verstanden werden. Anderenfalls können Serviceausfälle, ein vermindertes Sicherheitsniveau oder ungewollt hohe Kosten entstehen. Zu den wichtigsten Funktionen in diesem Zusammenhang zählen:

- Starten und Stoppen von Systemen
- Starten und Stoppen von Diensten
- Einrichtung von Benutzerkonten
- Änderungen an Berechtigungen für Benutzerkonten
- Änderungen am Logging
- Änderungen an Zugriffskontrolllisten
- Änderung der Bezeichnung von Systemen
- Änderung der zugewiesenen IP-Adressen
- Patchen von Systemen
- Änderungen von Speicherzuweisungen
- Ausführung von Programmen, die mit erweiterten Rechten laufen.

Graphische Administrationsoberfläche für Kunden

Das Dashboard, die graphische Administrationsoberfläche für Kunden, bietet Administratoren der von Kunden genutzten Cloud-Services eine webbasierte Oberfläche zur Bereitstellung und zum Zugriff auf Cloud-basierte Ressourcen. Das Dashboard kommuniziert mit den Back-End-Diensten der GRASS-MERKUR-Cloud über Anrufe an das Application Programming Interface (API).

Fähigkeiten des Dashboard

- Das Dashboard fungiert als ein Self-Service-Portal, mit Hilfe dessen Kunden sämtliche eigenen Cloud-Ressourcen innerhalb der von Administratoren festgelegten Grenzen verwalten können. Entscheidend für den Umfang der Gestaltungsmöglichkeiten an den Ressourcen der Cloud-Services sind die dem angemeldeten Benutzerkonto vorab zugewiesenen Rechte. Insbesondere können durch ungeeignete Benutzung den Kunden ungewollte Kosten entstehen oder das Sicherheitsniveau ungewollt herabgesetzt werden.
- Das Dashboard biete den Administratoren der Kunden eine Gesamtansicht des Umfangs der Nutzung und des Zustands ihrer in Anspruch genommenen Cloud-Services.
- Das Dashboard kann auch optisch für Kunden angepasst werden.

Sicherheitsaspekte des Dashboard

- Das Dashboard benötigt auf Kundenseite Cookies und JavaScript, um im Webbrowser aktiviert zu werden.
- Der Webserver auf GRASS-MERKR-Seite, der das Dashboard bereitstellt, ist ausschließlich für TLS-Kommunikation konfiguriert, um sicherzustellen, dass der Zugriff und übertragene Daten verschlüsselt sind.
- Sowohl der Web-Service als auch das API, das es verwendet, um mit dem Back-End innerhalb der GRASS-MERKUR-Cloud zu kommunizieren, sind anfällig für Web-Angriffsvektoren und werden deshalb intensiv überwacht.

4.35 Monitoring und Logging der Cloud-Services

GRASS-MEKRUR überwacht die Infrastruktur der GRASS-MERKUR-Cloud laufend auf Erreichbarkeit, Verfügbarkeit der Services, Kapazitätsauslastungen und bestimmte Systemzustände. Die Netzwerkverbindungen, die in der Verantwortung von GRASS-MERKUR liegen, werden ebenso überwacht. Gleiches gilt für die redundant ausgelegte Anbindung an das Internet. Netzfilter und Netztrennelemente sind in die Datenübertragungswege geschaltet und untersuchen bzw. filtern den Datenverkehr auf mehreren Schichten der Netzwerkprotokolle. In einem zentralen Monitoring- und Management-System werden die Messwerte und Beobachtungen korreliert, aggregiert und bewertet. Besondere Beachtung schenkt GRASS-MERKUR dabei der Vorbeugung und Entdeckung von Sicherheitsvorfällen, der missbräuchlichen Nutzung von Cloud-Systemen durch Dritte und der Detektion von Datenschutzverletzungen.

Auf die Überwachungstechnik, deren Parametrierung und die Auswertungsmöglichkeiten haben nur Administratoren der GRASS.MEKRUR Zugriff.

Zur Überwachung seiner genutzten Cloud-Services werden den Kunden folgende Möglichkeiten gegeben.

A) Zum einen kann ein Kunde die für die Services durch GRASS-MERKUR verfügbar gemachten Messgrößen (z.B. CPU-Auslastung, Speicherfüllstände, Performance-Werte, Netzwerkauslastung) und Messwerkzeuge nach eigenem Ermessen konfigurieren und sich über Abweichungen von Normalzuständen als Events informieren lassen.

B) Zum anderen können sich Kunden eine eigene zentrale Monitoring-Umgebung innerhalb der GRASS-MERKUR-Cloud einrichten und dadurch ihre eine Überwachungssystematik aufbauen und sich Events nach außerhalb der Cloud signalisieren lassen.

Es ist dabei immer sichergestellt, dass nur Messgrößen und zu beobachtende Systeme des jeweiligen Kunden überwacht werden können. Kunden können Zugriffsrechte auf das Monitoring selbst verwalten.

GRASS-MERKUR empfiehlt Kunden darüber hinaus den Einsatz von hostbasierten Intrusion Detection Systemen in Erwägung zu ziehen, falls erhöhte Sicherheitsanforderungen vorliegen. Solche Systeme sind hochgradig implementierungsspezifisch und werden deshalb von GRASS.MERKUR nicht standardmäßig eingesetzt.

GRASS-MERKUR-Cloud-Audit-Funktion.

Eine Auditierung der Aktivitäten, die durch Kundenmitarbeiter an den genutzten Cloud-Service vorgenommen wurden, ist möglich. Eine aussagekräftige, umfangreiche Logging-Funktion, die durch den Kundenadministrator in ihrem Umfang einstellbar ist, liefert Informationen darüber, welcher Service, zu welchem Zeitpunkt von welchem Benutzerkonto und welche Aktion ausgeführt wurde. Erfasst wird, ob die Aktion von einer Management-Konsole, durch die Kommandozeile oder durch ein System ausgeführt wurde.

Erfasst werden sämtliche Anmeldungen an der GRASS-MERKUR-Cloud. Gescheiterte Anmeldeversuche und fehlerhaft ausgeführte Operation werden protokolliert und ausgewiesen. Die so gesammelten Informationen werden dauerhaft gespeichert (jedoch längstens für 12 Monate), können aber per Kundenvorgabe nach einer bestimmten Zeit gelöscht, bzw. überschrieben werden. Der Zugriff und die Einsehbarkeit der Logging-Informationen können auf bestimmte Rollen/Benutzer eingeschränkt werden.

4.36 Sicherheit der virtuellen und physischen Netzwerke

Die GRASS-MERKUR Cloud-Services bieten Cloud-Nutzern verschiedene Netzwerkdienste wie IP-Adressverwaltung, DNS, DHCP, Load Balancing und Netzwerkzugriffsregeln wie Firewall-Richtlinien. Die Services bieten einen Rahmen für Software-definierte Vernetzung (SDN), für den adäquate Betrieb vormals von Kunden in eigener Hoheit betriebener Systeme in der GRASS-MERKUR-Cloud. Die Gestaltungsmöglichkeiten gestatten es Cloud-Kunden in einem gewissen Umfang, ihre Gast-Netzwerk-Konfigurationen selbst unter Berücksichtigung der Anforderungen an Netzverkehrs-Isolation, Verfügbarkeit, Integrität und Vertraulichkeit sowie Datenschutzaspekten zu planen, einzurichten und langfristig zu verwalten.

5 Servicespezifische IT-Sicherheitsaspekte

5.1 Speicherservices (Storage)

5.1.1 Objectstorage (GM-OBJECTSTOR)

GM-OBJSTOR stellt Speicherbereiche als Object-Storage-Container zur Verfügung. Kunden der GRASS-MERKUR-Cloud haben nur Zugriff auf ihre eigenen GM-OBJSTOR-Container. Zudem kann der Zugriff auf jeden einzelnen Container vom Kunden selbst abgestuft geregelt (schreiben/lesen) werden. Der Zugriff erfolgt ausschließlich über https-Verbindungen.

Im GM-OBJSTOR werden Daten in einer organisatorischen Hierarchie gespeichert, die Nur-Lese-Zugriff, Access-Control-Listen-definierten Zugriff oder auch nur temporären Zugriff bietet. GM-OBJSTOR unterstützt mehrere Authentifizierungsmechanismen, die über Middleware implementiert werden.

Anwendungen speichern Daten in GM-OBJSTOR und rufen diese über eine branchenübliche HTTP RESTful API ab und verbinden sich mit GM-OBJSTOR über technische Benutzerkonten. Back-End-Komponenten von GM-OBJSTOR folgen dem gleichen RESTful-Modell.

5.1.2 Blockstorage (GM-BLOCKSTOR)

Mit GM-BLOCKSTOR werden Kunden Speichervolumes für die Anbindung an Compute-Instanzen bereitgestellt. Diese Speichervolumes verhalten sich wie unformatierte Blockgeräte mit benutzerdefinierten Gerätenamen und einer Blockgeräteschnittstelle. Die Kunden können diese wie eine Festplatte verwenden und ein Dateisystem auf den Volumes erstellen. Der Zugriff auf GM-BLOCKSTOR ist nur für den Kunden möglich, dessen zugeordnetes Benutzerkonto das Volume angelegt hat. Das Recht zum Anzeigen oder Zugreifen auf das Volume kann der Kunde seinen eigenen Benutzerkonten selbst granular vergeben.

In GM-BLOCKSTOR gespeicherte Daten werden im Rahmen des normalen Betriebs nur einfach ohne Redundanz (z.B. Spiegelung) gespeichert. Die Einrichtung einer Redundanz ist durch Kunden explizit zu beantragen.

GRASS-MERKUR empfiehlt regelmäßige Snapshots oder Datensicherungen des GM-OBJECTSOR durchzuführen, um eine Datenwiederherstellbarkeit im Fehlerfall zu gewährleisten.

GM-BLOCKSTOR-Volumes werden Kunden als unformatierte Blockgeräte angezeigt, die vor der Bereitstellung zur Verwendung gelöscht wurden. Der Löschvorgang erfolgt unmittelbar vor der Wiederverwendung, sodass die Kunden sicher sein können, dass der Löschvorgang abgeschlossen ist. Hat ein Kunde den Bedarf des Löschens mit einer besonders sicheren Methode, sollte der Kunde auf GRASS-MERKUR zukommen und die Umsetzung dessen besprechen.

Sollten die auf GM-BLOCKSTOR abzulegenden Daten eine hohe Schutzstufe haben, rät GRASS-MERKUR dazu, die Daten vor der Ablage durch den Kunden selbst zu verschlüsseln. Empfohlen wird hierzu der Einsatz von AES-256.

5.2 Datensicherungsservices

5.2.1 GM-Direct Cloud-Backup

GM-Direct Cloud-Backup ist ein Service für die Datensicherung, wobei das Sicherungsmedium ein GM-

OBJSTOR in der GRASS-MERKUR-Cloud ist. Die Daten werden auf Kundenseite vor der Übertragung verschlüsselt. Die Übertragung erfolgt via https. Als Übertragungsweg zwischen Kundenlokation und GRASS-MERKUR-Cloud kann das Internet, eine VPN-Verbindung oder eine dedizierte Leitung genutzt werden. Die zu sichernden Clients auf Kundenseite müssen in der Lage sein, auf den Object Storage direkt schreibend und lesend zugreifen zu können. GRASS-MERKUR greift in die Verschlüsselung nicht ein, sondern erhält bereits verschlüsselte Daten, die im OBJSTOR abgelegt werden. Die Ver- und Entschlüsselung erfolgen ausschließlich auf der Seite des Kunden.

5.2.2 GM-Backup Cloud Boost

GM Backup Cloud Boost ist ein Service für die Datensicherung, wobei das Sicherungsmedium ein GM-OBJSTOR in der GRASS-MERKUR-Cloud ist. Die Daten werden auf Kundenseite vor der Übertragung verschlüsselt. Die Übertragung erfolgt via https. Als Übertragungsweg zwischen Kundenlokation und GRASS-MERKUR-Cloud kann das Internet, eine VPN-Verbindung oder eine dedizierte Leitung genutzt werden. Auf Kundenseite ist in die Backup-Infrastruktur ein als Appliance oder als Virtuelle Maschine implementiertes System zu ergänzen, das die Rolle eines Gateways zwischen der Backup-Umgebung des Kunden und dem GM-OBJSTOR einnimmt.

Die am Markt etablierten Backup-Lösungen verfügen sämtlich über ein solches Gateway in der Regel mit folgenden Funktionen:

- Deduplizierung, Kompression, Verschlüsselung
- Durchleitung der Backup-Daten in die Cloud
- Steuerung der Langzeitaufbewahrung
- Cloning der Backup-Daten
- Lokales Cachen der Backup-Daten

5.3 Rechenleistungsservices (Compute)

Die GM-Compute-Services sind virtuelle Server in der Cloud mit verschiedenen Betriebssystemen. Diese virtuellen Server können von Kunden aus einer Reihe von vorgegebenen und von GRASS-MERKUR vorkonfigurierten und dem geplanten Einsatzzweck entsprechend gehärteten Mustern abgeleitet und als eigenständige Instanzen aktiviert werden. Die Muster liegen in verschiedenen Ausstattungsvarianten (sog. Flavors) vor (CPU und RAM), im Weiteren bezeichnet als Instanz-Typen. Daneben besteht für Kunden aber auch die Möglichkeit einer in gegebenen technischen Grenzen freien Kombination von Leistungsparametern der Server. Die Kunden erhalten an diesen Instanzen den vollständigen administrativen Zugang. Wenn ein Kunde an einem Server das initial gesetzte Passwort für den Administrator/Root- Account ändert, was zu veranlassen ist, verfügt GRASS-MERKUR nicht mehr über den administrativen Zugang zu den Systemen. Durch Netzwerkkonfiguration kann die Erreichbarkeit der Server aus dem Internet oder ausschließlich im privaten Netzwerk der Kunden eingerichtet werden.

Sicherheitsschichten

Die Sicherheit von Serverinstanzen erstreckt sich über mehrere Ebenen: Das Betriebssystem der Host-Plattform (Hypervisor), das Betriebssystem der virtuellen Instanz (Gastsystem) und eine Firewall. Jede dieser Schichten baut auf den Sicherheitsfähigkeiten der anderen auf. Ziel ist es, die in der GRASS-MERKUR-Cloud enthaltenen Kundendaten vor nichtautorisierten Zugriffen zu schützen und die Server Instanzen selbst so sicher wie möglich bereitzustellen und zu betreiben, ohne die Flexibilität und Konfigurierbarkeit einzuschränken.

Instanz-Isolierung

Verschiedene Instanzen, die auf derselben physischen Maschine ausgeführt werden, werden über den Hypervisor voneinander isoliert. GRASS-MERKUR steht mit den Herstellern der Infrastrukturkomponenten in Kontakt und die Cloud-Architekten sind für die neuesten Entwicklungen informiert. Als technische Maßnahme befindet sich eine Firewall innerhalb der Hypervisor-Schicht zwischen der physischen Netzwerkschnittstelle und der virtuellen Schnittstelle der Sever-Instanz. Alle Neztwerk-Pakete müssen diese Schicht durchlaufen, daher haben die Nachbarn einer Instanz keinen Zugriff auf diese Instanz und können praktisch so betrachtet werden, als befänden sie sich auf separaten physischen Hosts. Der physische RAM wird unter Verwendung ähnlicher Mechanismen getrennt.

Kundeninstanzen haben keinen Zugriff auf Raw-Festplattengeräte, sondern werden mit virtualisierten Festplatten verbunden. Die Datenträgervirtualisierungsschicht der Cloud-Infrastruktur setzt bei Nutzungsbeendigung automatisch jeden vom Kunden verwendeten Speicherblock zurück, sodass die Daten eines Kunden niemals unbeabsichtigt einem anderen Kunden zugänglich sein werden. Außerdem wird der den Gastsystemen zugewiesene Speicher automatisch vom Hypervisor bereinigt (Scrubbing), wenn dieser von einem Gastsystem entfernt wird. Der Speicherbereich wird erst nach Beendigung des Scrubbing endgültig in den Pool des für neue Zuweisungen verfügbaren freien Speichers zurückgegeben.

GRASS-MERKUR empfiehlt den Kunden über dies die Dateisysteme der Server zu verschlüsseln.

Host-Betriebssystem

Administratoren der GRASS-MERKUR, die auf die Verwaltungsebene der Cloud-Infrastruktur zugreifen müssen, nutzen dazu Systeme, die speziell zum Schutz der Verwaltungsebene der Cloud entwickelt, konfiguriert und gehärtet werden. Alle diese Zugriffe werden protokolliert und geprüft. Wenn ein Cloud-Administrator nicht länger auf die Verwaltungsebene zugreifen muss, können dessen Berechtigungen und der Zugriff auf diese Hosts und relevanten Systeme widerrufen werden.

Gastbetriebssystem:

Virtuelle Instanzen werden vollständig vom Kunden, gesteuert. Kunden haben vollständigen Administrator, bzw. Root-Zugriff über die Benutzerkonten, die Dienste und Anwendungen. GRASS-MERKUR hat keine Zugriffsrechte für auf die Kunden-Server-Instanzen oder das Gastbetriebssystem. GRASS-MERKUR empfiehlt die Umsetzung von Best Practices für die Sicherheit, wie z.B. ausschließlich den zertifikatbasierten Zugriff auf Server-Instanzen per SSH Version 2 zuzulassen und das grundsätzliche Härten des Serverbetriebssystems.

Es wird empfohlen, die Befehlszeilenprotokollierung zu verwenden und "sudo" für Ausführung privilegierter Systemprogramme unter Linux zu nutzen. Remoteverbindungen zu Windows-Instanzen sollten mithilfe von Remote Desktop Protocol (RDP) hergestellt werden, wobei ein RDP-Zertifikat Verwendung finden sollte, das für die jeweilige Instanz generiert wurde.

Die Kunden steuern das Aktualisieren und Patchen Ihres Gastbetriebssystems vollständig selbst, einschließlich Sicherheitsupdates. Von GRASS-MERKUR bereitgestellte Windows- und Linux-basierte Muster (Images) werden regelmäßig mit den neuesten Patches aktualisiert:

Firewall:

Zwischen den Netzbereichen verschiedener Kunden zum Internet und zu den internen Systemen der GRASS-MERKUR sind Firewalls geschaltet. Firewalls sind grundsätzlich im Modus "deny all" konfiguriert, d.h. die Firewall verweigert alle Verbindungen und gewollte Verbindungen durch die Firewall müssen explizit geöffnet werden. Der Datenverkehr kann über das Protokoll, den Service-Port sowie die Quell-IP-Adresse (individuelle IP oder Adressbereiche) gesteuert werden.

Die Firewall kann in Gruppen konfiguriert werden, die unterschiedlichen Klassen von Instanzen unterschiedliche Regeln erlauben. Zum Beispiel für den Fall einer traditionellen dreistufigen Webanwendung. Die Gruppe für die Webserver hat Port 80 (HTTP) und / oder Port 443 (HTTPS) für das Internet geöffnet. Die Gruppe für die Anwendungsserver würde z.B. den anwendungsspezifischen Port 8000 nur für die Webservergruppe verfügbar machen. Die Gruppe für die Datenbankserver würde nur den Port 3306 (MySQL) nur

für die Anwendungsservergruppe öffnen. Alle drei Gruppen erlauben einen administrativen Zugriff auf Port 22 (SSH), jedoch nur aus dem Firmennetzwerk des Kunden heraus. Mit einer derartigen Konfiguration können beispielsweise hochsichere Anwendungen betrieben werden.

GRASS-MERKUR empfiehlt darüber hinausgehend auf den einzelnen Server-Instanzen zusätzliche Sicherungsmechanismen wie lokale Firewalls (IPtables oder Windows Firewall), VPNs oder intrusion detection Systeme zu implementieren.

6 Mitgeltende Dokumente

- GRASS-MERKUR - Leitlinie-Cloud-Datenschutz

7 Revision

Die Historie wird nach unten fortgeschrieben.

Version	Stand	Autor	Änderungen
v0.1.0	20180426	Dr. Oliver Kunert	initiale Version, Entwurf
v0.2.0	20190701	Dr. Oliver Kunert	Anpassungen nach endgültigem Zuschnitt der GM-Cloud-Services
v1.0.0	20190712	Jochen Kaiser	Freigabeversion