Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK
Bereich Digitale Transformation und IKT-Lenkung DTI

AR012 – Architekturrichtlinie für den Identitätenschutz - Beilage 1

Beilage zu einer IKT-Vorgabe

Sachtitel (der Beilage):	**Schichten-Modell MCT**
Ausgabedatum dieser Beilage:[1]	17. August 2023
Gehört zu:	AR012, Version 1.0
Status der Weisung:	Genehmigt

[1] Das *Ausgabedatum* stimmt bei der Erstpublikation einer Beilage mit dem *Beschlussdatum* der genehmigten Version einer Weisung zur Bundesinformatik überein. Bei einer geringfügigen Änderung in der Beilage wird auf eine Anpassung der Version der Weisung verzichtet. Es ist lediglich das *Ausgabedatum* der Beilage anzupassen sowie die Änderung in *Anhang A der Beilage* festzuhalten.

Inhaltsverzeichnis

1 Allgemeine Bestimmungen

1.1 Gegenstand

1. Dieses Dokument ist eine Beilage der Architekturrichtlinie für den Identitätenschutz und regelt die Grundsätze und Gestaltungsprinzipien für das Schichten-Modell.

1.2 Geltungsbereich

1. Der Geltungsbereich dieser IKT-Vorgabe ist identisch mit dem Geltungsbereich des Hauptdokuments. Die Verbindlichkeitsgrade sind auch anzuwenden.

1.3 Begriffe

a. In dieser IKT-Vorgabe bedeuten (→ weitere Definitionen befinden sich im Hauptdokument)
   a. ***Tier**:* Die Definition befindet sich im Hauptdokument.
      Tier und Schicht können synonym gebraucht werden. Aus Verständlichkeitsgründen wird im Kontext MCT der Begriff «Tier» bevorzugt verwendet.
   b. ***Login/Logon:*** Der Prozess bei dem ein menschlicher oder technischer Nutzer Zugriff auf ein System erlangt.
   c. **Schutzobjekt**: Die Definition befindet sich im Hauptdokument.

2 Schichtenmodell (Tier-Modell)

2.1 Ausgangslage

Ohne ergänzende Sicherheitsmassnahmen besteht die Gefahr, dass Angreifer Credentials entwenden und sich durch «Lateral Movement» (Seitwärtsbewegung) und «Privilege Escalation» (Erarbeiten höherer Berechtigungen) bis hin zu administrativen Privilegien hocharbeiten.

Nebst der Einführung einer PAM-Lösung über die gesamte IKT Infrastruktur (*vgl. «Referenz Architekturprinzipien [PAM]»*) muss gewährleistet sein, dass sich privilegierte Accounts nur in einem vordefinierten Rahmen bewegen können. Hierfür hat *Microsoft* ein Schichten-Modell (-Tier-Modell) entwickelt, welches privilegierte Accounts je nach Kritikalität in verschiedene Schichten aufteilt. Das Tier-Modell, resp. dessen Grundsätze, sind nicht auf Microsoft-Infrastrukturen beschränkt und es empfiehlt sich, das Modell auf die gesamte IKT-Landschaft anzuwenden.

Privilegierte Accounts dürfen sich gemäss des Tier-Modells nur innerhalb einer dieser Schichten an Systemen anmelden, sodass Missbrauch in anderen Tiers grundsätzlich verhindert werden kann. Eine Anmeldung auf Systemen, die nicht demselben Tier angehören, ist technisch zu verhindern.

Nachfolgend werden die Ziele, Grundsätze und Prinzipien dieses Schichten-Modells, im Kontext «WAS» will man, beschrieben. Das vorliegende Dokument soll bei der Einführung des Schichten-Modells als Grundlagendokument zur Hilfestellung und als Referenz dienen.

3 Architekturprinzipien Schichtenmodell

Nachfolgende Architekturprinzipien gelten für die Büroautomation und MÜSSEN zwingend angewendet werden. Ausserhalb der Büroautomation sollen ein Schichtenmodell und die nachfolgenden Architekturprinzipien nach besten Möglichkeiten umgesetzt werden.

Nr.	**1**	Titel	**Zuordnung von Systemen in Schichten**
Aussage (Prinzip)			IT-Systeme MÜSSEN immer eindeutig einer bestimmten Schicht (Tier) zugeordnet werden. (Beispiel BA-Client / APS = Schicht 2).
Begründung			Durch die Zuordnung von Systemen zu einer Schicht wird sichergestellt, dass eine konforme Administration möglich ist und nicht schichtübergreifend administriert werden muss. Es ist im Weiteren sicherzustellen, dass Systeme – wenn diese keiner Schicht zugeordnet sind – NICHT administriert werden können.
Auswirkung			Bei der Definition von IT-Services muss eine Zuordnung von Systemen in Schichten oder dedizierte Administrationsbereiche erfolgen.
Bemerkungen			Zu berücksichtigen ist hierzu vgl. Kapitel 3.3 «Account Typen und Schichtenmodell». Basierend auf Prinzip 2 «Least Privilege», s. Hauptdokument AR012

Nr.	**2**	Titel	**Zuordnung von privilegierten Accounts zu Schichten**
Aussage (Prinzip)			Ein privilegierter Account MUSS immer genau einer Schicht zugeordnet werden. Der Isolationsbereich und der Einsatzbereich privilegierter Credentials MUSS so klein wie möglich und so gross wie nötig gehalten werden. Evtl. sind ergänzend entsprechende isolierte Server- oder Service-Silos im Tier0 zu bilden oder eine 1:1 Beziehung System/Credential (z.B. LAPS Credentials aus T0 DÜRFEN NICHT auf Systemen anderer Schichten zu liegen kommen. Dies ist technisch (z.B. Deny Logon) sicherzustellen.
Begründung			Um «Privileged Escalation» vorzubeugen, müssen privilegierte Accounts stets einer konkreten Schicht zugeordnet werden.
Auswirkung			Privilegierte Accounts sind immer fest einer einzigen Schicht zuzuordnen und können nicht schichtenübergreifend eingesetzt werden. Sofern eine Rolle in einer anderen Schicht ebenfalls benötigt wird, ist diese parallel zu erstellen oder die Rolle ist in der einen Schicht zu löschen und in der neuen Schicht neu zu etablieren.
Bemerkungen			Zu berücksichtigen ist hierzu Kapitel 3.3 «Account Typen und Schichtenmodell». Basierend auf Prinzip 2 «Least Privilege», s. Hauptdokument AR012

Nr.	**3**	Titel	**Schichtentrennung auf Physik/Host-Ebene**
Aussage (Prinzip)			Sofern mittels technischer Massnahmen (z.B. shielded VMs, Verschlüsselung, etc.) nicht sichergestellt werden kann, dass ein schichten- oder systemübergreifender Zugriff verhindert ist, MUSS eine Trennung auf Physik/Hostebene erfolgen.
Begründung			Dem Risiko, dass von einem Gast-System einer tieferen Schicht auf das Gast-System einer höheren Schicht zugegriffen werden kann, ist konsequent entgegenzuwirken. (z.B. Intel Spectre).
Auswirkung			Im On-Premises Umfeld ist die Verwendung dedizierter physischer Hosts pro Schicht oder analoge technische Massnahmen, umzusetzen.
Bemerkungen			Basierend auf Prinzip 3 «Clean Source» und Prinzip 1 «Zero Trust», s. Hauptdokument AR012

Nr.	**4**	Titel	**Getrennte Administrations- und Managementsysteme pro Schicht**
Aussage (Prinzip)			Es MUSS zu jedem Zeitpunkt sichergestellt werden, dass sich privilegierte Credentials auf Administrationsgeräten nicht überschneiden. Kann dies nicht mittels geeigneter Massnahmen garantiert werden, so ist konsequenterweise ein dediziertes Administrationssystem je Schicht einzusetzen.
Begründung			Credentials aus unterschiedlichen Schichten DÜRFEN NICHT auf denselben Administrationssystemen zum Liegen kommen. Sofern dies technisch nicht sichergestellt werden kann, sind dedizierte Konten und Administrationssysteme einzusetzen, da anderenfalls die Gefahr besteht, dass Dritte diese Systeme zur Kompromittierung mehrerer Schichten verwenden («Privilege Escalation»).
Auswirkung			Systeme müssen für die Administration einzelner Schichten zur Verfügung gestellt werden.
Bemerkungen			Alle Komponenten, die zu einer Kompromittierung eines Systems relevant sind, müssen der jeweiligen Schicht zugeordnet werden. Basierend auf Prinzip 2 «Least Privilege», s. Hauptdokument AR012

Nr.	**5**	Titel	**Gültigkeit des Schichten-Modells für die gesamte IKT**
Aussage (Prinzip)			Das Schichtenmodell hat Gültigkeit für alle IKT Plattformen und Systemlandschaften in der Bundesverwaltung und MUSS eingehalten werden. Die Zuordnung der IKT-Systeme hin zu den getrennten Schichten oder Isolationsbereichen im Schichtenmodell (Tier Model) ist in Kap. 3.2 beschrieben.
Begründung			Das Tier-Modell muss für die gesamte IKT Landschaft angewendet werden, damit es den gewünschten Sicherheitsgewinn erzielen kann. Auch Systeme Windows-fremder Plattformen

Nr.	**5**	Titel	**Gültigkeit des Schichten-Modells für die gesamte IKT**
			müssen ausreichend gegen Bedrohungen («Privilege Escalation») geschützt werden und sinngemäss das Model anwenden.
Auswirkung			Für alle IKT Systeme MUSS eine Zuordnung zu definierten Schichten oder Isolationsbereichen erfolgen. Es MUSS technisch sichergestellt werden, dass Credentials einer Schicht nicht in einer anderen Schicht angewendet werden können und niemals dort abgelegt werden.
Bemerkungen			

Nr.	**6**	Titel	**Das Schichtenmodell adressiert die Zugriffe von privilegierten Credentials**
Aussage (Prinzip)			Die Kommunikation zwischen den Schichten ist nach wie vor vorgesehen und auch notwendig. Die Trennung der Schichten bezieht sich auf die Zugriffe der privilegierten Credentials zur Anmeldung/Administration/der Systeme, Dienste, Funktionen und Services.
Begründung			Das Schichtenmodell soll vor allem gegen Privilege Escalation-Methoden schützen.
Auswirkung			Die Kommunikation zwischen Systemen unterschiedlicher Schichten ist weiterhin zulässig. Eine administrative Tätigkeit innerhalb einer Schicht MUSS immer mittels eines privilegierten Accounts und Administrationsgerät in derselben Schicht ausgeführt werden. Ein privilegierter Benutzer DARF sich NICHT an einem System einer über- oder untergeordneten Schicht anmelden, weder interaktiv, noch mittels RDP oder als Dienst.
Bemerkungen			Basierend auf Prinzip 1 «Zero Trust», s. Hauptdokument AR012

Nr.	**7**	Titel	**Klassifizierung von Services zu den Isolationsbereichen (Schichten)**
Aussage (Prinzip)			Privilegierte Accounts (Security Principals), Systeme und Applikationen müssen einem Tier zugeordnet werden. Services, Service-Gruppen und Anwendungen sowie die Systeme, welche diese Funktionen bereitstellen, müssen einem Isolationsbereich (Schicht) zugewiesen werden.
Begründung			Diese Auslegeordnung muss vor Beginn gemacht werden und kann bei Bedarf erweitert werden.
Auswirkung			Auf Grund dieser Einordnung müssen in der Folge ebenfalls die privilegierten Accounts und Rollen den Schichten zugewiesen werden.
Bemerkungen			Zu berücksichtigen ist hierzu Kapitel «Account Typen und Schichtenmodell».

Nr.	7	Titel	**Klassifizierung von Services zu den Isolationsbereichen (Schichten)**
			Basierend auf Prinzip 2 «Least Privilege», s. Hauptdokument AR012

Nr.	8	Titel	**Berechtigungen technisch einschränken**
Aussage (Prinzip)			Es MUSS technisch sichergestellt werden, dass Credentials eines Tier nicht in einem anderen Tier angewendet werden können und niemals dort zu liegen kommen
Begründung			Dies dient der Verhinderung von Privilege Escalation.
Auswirkung			Das Rollenkonzept muss das Tiering berücksichtigen und unterstützen. Pro Rolle gibt es Verantwortliche, welche die Kontrolle und Verantwortung über die Berechtigungen haben müssen. Es müssen Control Restrictions eingeführt werden: Wer kontrolliert was. Es müssen Logon Restrictions eingeführt werden. Diese gelten primär für folgende Logon-Typen: Logon Locally Logon as Service Logon as Batch Job Logon through Remote Desktop Services.
Bemerkungen			Basierend auf Prinzip 2 «Least Privilege», s. Hauptdokument AR012

Nr.	9	Titel	**Anmeldungen überwachen und bei Missbrauch alarmieren**
Aussage (Prinzip)			Die technische Detektion und Alarmierung von Missbrauch und Unregelmässigkeiten innerhalb der administrativen Schichtentrennung muss etabliert werden.
Begründung			Die Detektion von und die Alarmierung bei Angriffen muss gewährleistet sein. Fehlerhafte oder versuchte Anmeldungen müssen genauso analysiert und einer Mustererkennung zugeführt werden wie erfolgreiche Anmeldungen.
Auswirkung			Eine vollumfängliche Nachvollziehbarkeit von der Nutzung von privilegierten Accounts über die gesamte IKT Landschaft (Logging).
Bemerkungen			Basierend auf Prinzip 1 «Zero Trust», s. Hauptdokument AR012

Nr.	**10**	Titel	**Verantwortliche Person pro Rolle**
Aussage (Prinzip)			Für jede Rolle gibt es eine verantwortliche Person, welche nebst der Rollenzugehörigkeit die Einhaltung der Prinzipien des Tier-Modells sicherstellt.
Begründung			Nur die verantwortliche Person kann beurteilen, ob die Rollenzugehörigkeit richtig gewählt wurde.
Auswirkung			Es braucht hierzu Regeln und Vorgaben zu den Rollen.
Bemerkungen			Basierend auf Prinzip 2 «Least Privilege», s. Hauptdokument AR012

Nr.	**11**	Titel	**Sicherheits-Baseline innerhalb einer Schicht**
Aussage (Prinzip)			Es MUSS zu jedem Zeitpunkt sichergestellt sein, dass die Systeme des Tier0 über eine aktuelle Security Baseline verfügen, die bezüglich der Einstellungen im Mindesten den Best Practices des Herstellers entspricht. Innerhalb einer Schicht müssen alle IKT-Komponenten eine definierte Sicherheits-Baseline aufweisen. Diese entspricht im Minimum der Sicherheits-Baseline des Herstellers und dessen Best Practices und ist regelmässig auf Übereinstimmung zu prüfen und zu aktualisieren.
Begründung			Falls innerhalb einer Schicht die Sicherheits-Baseline nicht gewährleistet ist, gefährdet dies andere Systeme und Services innerhalb des Tiers und suggeriert falsche Sicherheit.
Auswirkung			Die Sicherheits-Baseline der Systeme muss auf dem gleichen Level sein. Nachfolgende Punkte sind dabei durch den Sicherheitsverantwortlichen eines Leistungserbringers mindestens zu berücksichtigen: - Grundschutz - Hardening - Patchlevel - Clean Source
Bemerkungen			

4 Optional: Architektur Schichtenmodell (Tier-Modell)

Die in diesem Kapitel aufgeführten Gestaltungsprinzipien, Beschreibungen und Grundsätze sollen bei der Implementierung des Schichtenmodells und deren Nutzung berücksichtigt werden, stellen aber keine verpflichtenden Vorgaben dar.

Bei diesem Kapitel handelt es sich um eine Darstellung und Erklärung von Best-Practice Architekturen, die in der IT-Landschaft des Bundes berücksichtigt werden sollten, aber keine Vorgabe darstellt. Hierbei handelt es sich um eine Inspirationsvorlage / Empfehlung und nicht um eine Vorgabe.

4.1 Zielbild zur administrativen Schichtentrennung

Die wichtigste Grundlage, dem «Lateral Movement» und der «Privilege Escalation» in der Bundesverwaltung entgegenzuwirken, ist die Schaffung von geschützten Isolationsbereichen, die ausschliesslich durch Konten und Geräte desselben Isolationsbereichs administriert werden. Das Vorlagemodell von Microsoft sieht drei vollständig getrennte Schichten vor, sowie vollständig getrennte Privilegien und Administrationsgeräte für jede dieser Schichten.

Nachfolgend werden die Komponenten und deren Grundsätze, welche bei einem möglichen Tier-Modell zur Anwendung kommen können, grafisch dargestellt und textuell beschrieben.

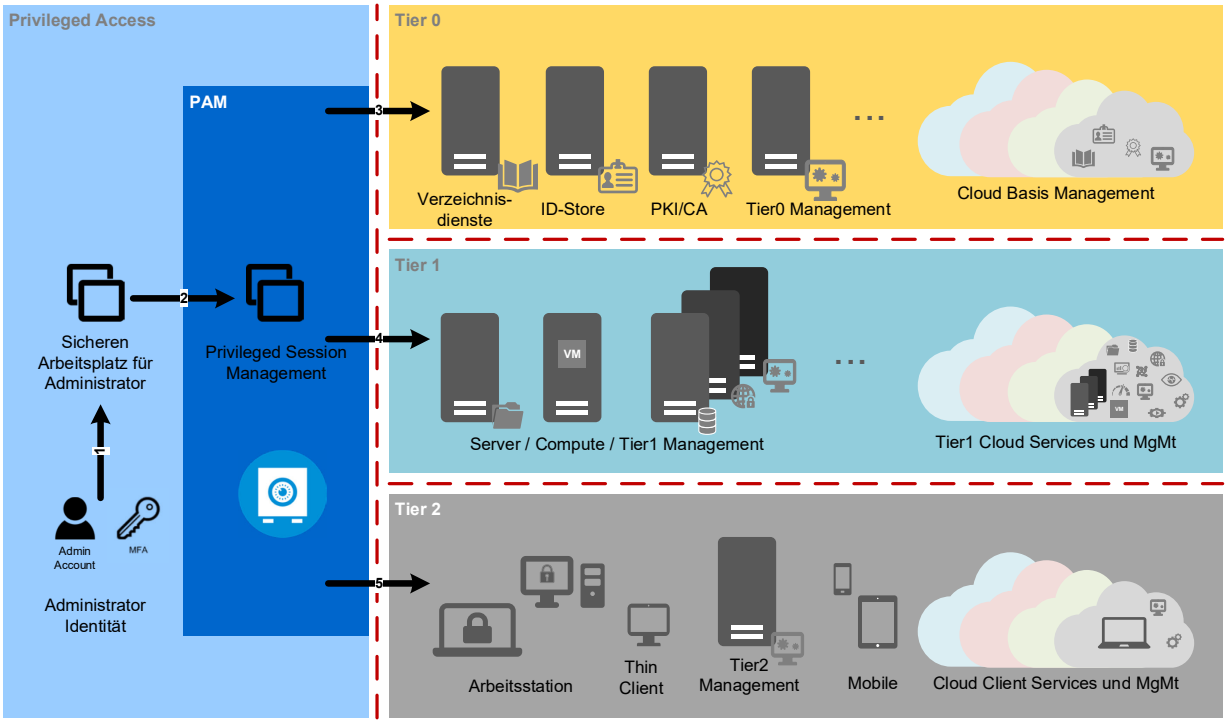

Abbildung 1: Ein Drei-Schichten-Modell inkl. Privileged Access (Three Tier Model) (Quelle: eigene Grafik)

Microsoft hat das «Schichten-Model» erweitert und in «*Enterprise Access Model*» umbenannt. Ebenfalls werden laufend neue Aspekte eingebracht, insbesondere die Verwaltung von Cloud-Diensten.

Im Microsoft «*Enterprise Access Model*» verwendet Microsoft neue Begrifflichkeiten. [2]

[2] *Vgl. Microsoft «Enterprise access model»:*

Nachfolgend sind die neuen Begrifflichkeiten in Bezug auf das Tier-Modell aufgeführt.
Wir behalten die Begrifflichkeit des ursprünglichen Tier-Modells bei, da diese aktuell besser verständlich ist und on-premises 1:1 klar adressiert und umgesetzt werden kann.

Die Administration von Cloud-Diensten muss mit dedizierten Konten erfolgen und stellt einen eigenen Isolationsbereich dar (eigene Schicht).

Beispiele für neue Begrifflichkeiten:

- «Control Plane» anstelle von Tier 0
- “Management Plane, Data/Workload Plane” anstelle von Tier 1
- “User Access, App Access” an Stelle von Tier 2

AR012 – Begriff	Microsoft Tiering	Microsoft Enterprise Access Model
PAM- Ebene	Bastion / Red Forest	Privileged Access
Tier 0	Tier 0	Control Plane
Tier 1		Management Plane
Tier 1	Tier 1	Data/Workload Plane
Tier 2	Tier 2	Access Plane

Tabelle 1: Zuordnung der Begriffe zwischen AR012 und anderen Modellen.

Da es unterschiedliche Implementation und Interpretationen des Schichten-Modells gibt, ist in Tabelle 1 eine Definition der Schichten (Tiers) eingefügt. Diese stellt die Zuordnung der in AR012 definierten und beschriebenen Schichten auf bekannte Modelle dar.

Im Folgenden werden die Komponenten des Tier-Modells einzeln erläutert.

Nr. 1	**Komponente**	**Privileged Access (PA)**
Beschreibung		Der privilegierte Zugang beschreibt, dass privilegierte Credentials sicher, geschützt, isoliert und nur über ein PAM Werkzeug automatisiert verwendet und verwaltet werden dürfen. Siehe hierzu «*Referenz Architekturprinzipien PAM*». Der «Privileged Access» kann als eigenes Tier 0 oberhalb oder parallel zum klassischen Tier 0 betrachtet werden. Aus diesem Grund sollen Komponenten daraus grösstenteils zusätzlich gesichert, isoliert und mit dedizierten Credentials betrieben werden.
Funktion		Sichere, geschützte, isolierte Verwendung von privilegierten Credentials, die nur in einem Isolationsbereich (Schicht) Anwendung finden.
Ausprägung		vgl. «*Referenz AR012-Beilage 2 Architekturprinzipien PAM*»
Anforderungen		vgl. «*Referenz AR012-Beilage 2 Architekturprinzipien PAM*»

- https://docs.microsoft.com/en-us/security/compass/privileged-access-access-model
- https://docs.microsoft.com/en-us/security/compass/media/privileged-access-strategy/legacy-tier-model-comparison-new.png

Nr. 2	**Komponente**	**Tier 0 *(Control Plane)***
Beschreibung		Tier 0 ist, abgesehen vom «Privileged Access», der oberste Layer des klassischen Schichtenmodells. Er isoliert darin die Systeme und Services und deren privilegierte Credentials gemäss Kapitel 3.3 «Account Typen und Schichtenmodell». Im Tier 0 befinden sich nebst dem «Privileged Access Management» (1) die hochkritischen Systeme und die damit verbundenen privilegierten Accounts.
Funktion		- Absicherung der privilegierten Credentials des Tier 0 - Sichere und isolierte Verwaltung von Tier 0-Services und -Systemen - Technisches Verhindern des Zugriffs aus anderen Isolationsbereichen oder Tiers (z.B. Tier1, Tier2).
Ausprägung		Im Tier 0 werden ausschliesslich identitätsstiftende oder –verwaltende Systeme sowie deren Begleit- oder Umsysteme verwaltet. Es ist stets darauf zu achten, dass Tier0 Credentials niemals auf Systemen anderer Isolationsbereiche oder Schichten zu liegen kommen oder abgegriffen werden können (z.B. über die Virtualisierungs- oder Management-Infrastruktur).
Anforderungen		Für die Tier 0-Systeme ist ein eigenes dediziertes Management erforderlich, damit über den Weg des Managements die privilegierten Tier 0-Credentials ebenfalls geschützt sind und nicht über ein unterliegendes Tier missbraucht werden können. Privilegierte Credentials im Tier 0 müssen so eingesetzt werden, dass ein lateral Movement verhindert werden kann. U.a. sollen privilegierte Accounts pro System lokal anstatt aus zentralen Verzeichnisdiensten stammende Accounts verwendet werden. Die Administration mit privilegierten Credentials erfolgt über den «Privileged Access» (1) gesichert und isoliert.

Nr. 3	**Komponente**	**Tier 1 *(Management Plane, Data/Workload Plane)***
Beschreibung		Das Tier1 ist eine weitere Schicht des klassischen Schichtenmodells, welcher primär das «Business» respektive die Bereiche Data und Workload beinhaltet. Es isoliert darin die Systeme und Services und deren privilegierte Credentials gemäss Kapitel 3.3 «Account Typen und Schichtenmodell».
Funktion		- Absicherung der privilegierten Credentials in Tier 1 - Sichere und isolierte Verwaltung von Tier 1-Services und -Systemen - Credentials aus T1 DÜRFEN NICHT auf Systemen anderer Schichten zu liegen kommen. Dies ist technisch (z.B. Deny Logon) sicherzustellen.
Ausprägung		Im Tier 1 werden primär Anwendungs- oder Datenhaltungssysteme resp. deren Credentials verwaltet. Die klassischen File-Services, Web- oder Datenbankserver werden typischerweise im Tier 1 verortet.
Anforderungen		Der Isolationsbereich und der Einsatzbereich privilegierter Credentials MUSS so klein wie möglich und so gross wie nötig gehalten werden. Evtl. sind ergänzend entsprechende isolierte Server- oder Service-Silos im Tier 1 zu bilden oder eine 1:1 Beziehung System/Credential (z.B. LAPS).

Nr. 3	Komponente	Tier 1 *(Management Plane, Data/Workload Plane)*
		Credentials aus Tier 1 DÜRFEN NICHT auf Systemen anderer Schichten zu liegen kommen. Dies ist technisch (z.B. Deny Logon) zu verhindern. Es MUSS zu jedem Zeitpunkt sichergestellt sein, dass die Systeme des Tier 1 über eine aktuelle Security Baseline verfügen, die bezüglich der Einstellungen im Mindesten den Best Practices des Herstellers entspricht.

Nr. 4	Komponente	Tier 2 *(User Access, App Access)*
Beschreibung		Im Tier 2 befinden sich die Clientsysteme und Enduser und deren Management-Infrastruktur. Er isoliert darin die Systeme und Services sowie deren privilegierte Credentials gemäss Kapitel 3.3 «Account Typen und Schichtenmodell».
Funktion		- Absicherung der privilegierten Credentials in Tier 2 - Sichere und isolierte Verwaltung von Tier 2-Services und -Systemen - Verhinderung, dass privilegierte Tier 2-Credentials offengelegt und missbraucht werden können
Ausprägung		Im Tier 2 wird typischerweise die Endbenutzer-Infrastruktur bereitgestellt und betrieben. Dennoch gibt es in diesem Bereich Credentials mit weitreichenden Berechtigungen auf zahlreichen Systemen (z.B. Rolle IT-Support).
Anforderungen		Der Isolationsbereich und der Einsatzbereich privilegierter Credentials MUSS so klein wie möglich und so gross wie nötig gehalten werden. Evtl. sind ergänzend entsprechende isolierte Client oder Server-Silos im Tier 2 zu bilden oder eine 1:1 Beziehung System/Credential (z.B. LAPS) Credentials aus Tier 2 DÜRFEN NICHT auf Systemen anderer Schichten zu liegen kommen. Dies ist technisch (z.B. Deny Logon) zu verhindern. Es MUSS zu jedem Zeitpunkt sichergestellt sein, dass die Systeme des Tier 2 über eine aktuelle Security Baseline (Client oder Server) verfügen, die bezüglich der Einstellungen im Mindesten den Best Practices des Herstellers entspricht.

Nr. 5	Komponente	Verzeichnisdienste, ID-Store, PKI/CA …
Beschreibung		Tier 0-Systeme führen und verwalten technische Identitäten sowie hochprivilegierte Schlüsselrollen.
Funktion		- Verwaltung von technischen Identitäten und Schlüsselrollen und hochkritischen identitätsstiftenden oder –verwaltenden Systemen.
Ausprägung		Vgl. Beilage 2 «*Architekturprinzipien PAM*»
Anforderungen		Je Systemtyp werden dedizierte Rollen nach dem «Least Privilege Prinzip» verwendet. Beispielsweise melden sich «Domain Admins» nur noch auf Domain Controllern und ihren gesicherten Adminsystemen (aka PAW) an.

Nr. 6	Komponente	Tier 0 Management
Beschreibung		Unter Tier 0 Management sind alle unterstützenden Systeme für Tier 0 (2) und «Privileged Access» (1) zu verstehen.
Funktion		- Sicheres und isoliertes Management von Tier 0-Services und -Systemen - Verhinderung, dass privilegierte Tier 0-Management-Credentials offengelegt und missbraucht werden können
Ausprägung		Es muss zu jedem Zeitpunkt sichergestellt sein, dass Credentials aus dem Management des Tier 0 nicht auf tieferliegenden Systemen oder in anderen Isolationsbereichen zu liegen kommen.
Anforderungen		Das Management für Tier 0 KANN isoliert oder in demselben Isolationsbereich wie der Tier 0 zu liegen kommen.

Nr. 7	Komponente	Cloud Basis Management
Beschreibung		Als Basis-Cloud-Service kann bspw. ein «Global Admin» im Azure AD oder der höchste Exchange Admin in M365, welcher wiederum die Exchange Admins verwaltet, verstanden werden.
Funktion		Absicherung der privilegierten Credentials und Schlüsselrollen des Cloud Basis Managements. Sichere und isolierte Verwaltung von Cloud-Rollen. Verhinderung, dass höchst privilegierte Cloud Credentials offengelegt werden und ggf. missbraucht werden könnten.
Ausprägung		Die Basis-Cloud-Management-Credentials sollten wenig zum Einsatz kommen. Sind die unterliegenden Rollen einmal zugeteilt und technisch umgesetzt, bedarf es dieses Basis-Cloud-Management-Credentials nur in seltenen Fällen. Die «Basis-Cloud-Services» von Public Clouds resp. deren Credentials müssen im Tier 0 verwaltet werden.
Anforderungen		

Nr. 8	Komponente	Server / Computer / Tier 1 Services
Beschreibung		Server-Systeme, deren Rechenleistung, Dienste, Funktionen und Services für Tier 1 bereitgestellt wird. Typischerweise wird diese Schicht als «Business Layer» oder mit Data/Workload bezeichnet, da sich in diesem die Fachanwendungs- und Datenhaltungssysteme befinden.
Funktion		Bereitstellen von Rechenleistung, Daten und Diensten, Funktionen und Services für Tier 1
Ausprägung		vgl. Kapitel 3.3 «Account Typen und Schichtenmodell».
Anforderungen		

Nr. 9	**Komponente**	**Tier 1 Management**
Beschreibung		Unter Tier 1 Management sind alle unterstützenden Systeme für Tier 1 (3) zu verstehen.
Funktion		- Sicheres und isoliertes Management von Tier 1-Systemen, -Diensten, -Funktionen und -Services - Verhinderung, dass privilegierte Tier 1 Management Credentials offengelegt und missbraucht werden können
Ausprägung		Das Management für Tier 1 KANN isoliert oder in demselben Isolationsbereich wie der Tier 1 zu liegen kommen.
Anforderungen		

Nr. 10	**Komponente**	**Tier 1 Cloud Services**
Beschreibung		Im Tier 1 werden Cloud Services bereitgestellt und verwaltet. Hier werden privilegierte Credentials für die tägliche Verwaltung dieser Services verwendet.
Funktion		Sichere und isolierte Verwaltung und Management von Tier 1 Cloud Services
Ausprägung		vgl. Kapitel 3.3 «Account Typen und Schichtenmodell».
Anforderungen		Eine Vertiefung der Cloud-Aspekte wird zu einem späteren Zeitpunkt ergänzt.

Nr. 11	**Komponente**	**Endgeräte und Endbenutzer,**
Beschreibung		Im Tier 2 befinden sich die Endgeräte und die Endbenutzer. Dies beinhaltet sowohl die Arbeitsstationen, Thin Clients, wie auch die mobilen Geräte wie Handys, Tablets etc.
Funktion		Bereitstellen von Endgeräten und Identitätsreferenzen (Benutzeraccounts) für Bundesmitarbeiter und Externe (Endbenutzer)
Ausprägung		vgl. Kapitel 3.3 «Account Typen und Schichtenmodell».

Nr. 12	**Komponente**	**Tier 2 Management**
Beschreibung		Unter Tier 2 Management sind alle unterstützenden Systeme für Tier 2 (4) zu verstehen.
Funktion		Sicheres und isoliertes Management von Tier 2-Systemen, -Diensten, -Funktionen und Services. Provisionierung von Endgeräten und Endbenutzerobjekten. Konten und Rollen, die für den Betrieb der Endbenutzerinfrastruktur notwendig sind (z.B. Service Desk, Support, etc.)
Ausprägung		
Anforderungen		Verhinderung, dass privilegierte Tier 2 Management Credentials offengelegt und missbraucht werden können. Verhinderung von «Lateral Movement» ist hierbei extrem wichtig.

4.2 Zusammenspiel der Schichten

In den Abbildungen 2, 3 und 4 wird das Zusammenspiel der Schichten grob erklärt:

Das Schichtenmodell sorgt dafür, dass in der jeweiligen Schicht ausschliesslich die darin benötigten privilegierten Benutzer und Administrationskonten getrennt oder, wenn notwendig, isoliert geführt sind und die privilegierten Credentials (wie administrative Kennungen) isoliert angewendet werden (Same Tier Logon; grüner Pfeil).

Die Administration von IKT-Systemen, Diensten, Funktionen und Service erfolgt konsequent mit Konten und Administrationssystemen aus derselben oder einer gleichgestellten Schicht. Privilegierte Zugriffe aus einer Schicht auf Systeme übergeordneter Schichten sind verboten. (bspw. von Schicht 1 nach Schicht 0; gelber Pfeil). Dasselbe gilt für unterliegende Schichten (roter Pfeil).

Ein Domain Admin darf sich demnach maximal nur an Geräten der Schicht 0 anmelden (Login), nicht aber an Servern der Schicht 1 oder Endbenutzergeräten (Workstations, APS) der Schicht 2 (Lower Tier Logon; roter Pfeil). Dies ist technisch sicherzustellen.
Umgekehrt dürfen ein Workstation-Administrator oder ein Standardbenutzer sich mit ihrer Kennung nicht an Geräten der Schicht 1 und Schicht 0 interaktiv anmelden (Login). Eine Anmeldung zur Nutzung eines Dienstes (logon over the network) ist selbstverständlich zulässig. Durch dieses Anmeldeverfahren werden keine Credentials auf den Zielsystemen zwischengespeichert.

Innerhalb des Login-Prozesses bspw. eines Benutzers an einem APS darf bspw. dennoch auf ein Active Directory zugegriffen werden. Dies ist notwendig und wird durch gesonderte Mechanismen gesichert (Service-Nutzung, Higher Tier Logon; gelber Pfeil).

Durch die Umsetzung dieser administrativen Schichtentrennung (siehe Abbildung 2) wird verhindert, dass administrative Kennungen der einen Schicht einen Zugang in andere Schichten öffnen und eine Eskalation der Privilegien ermöglichen.

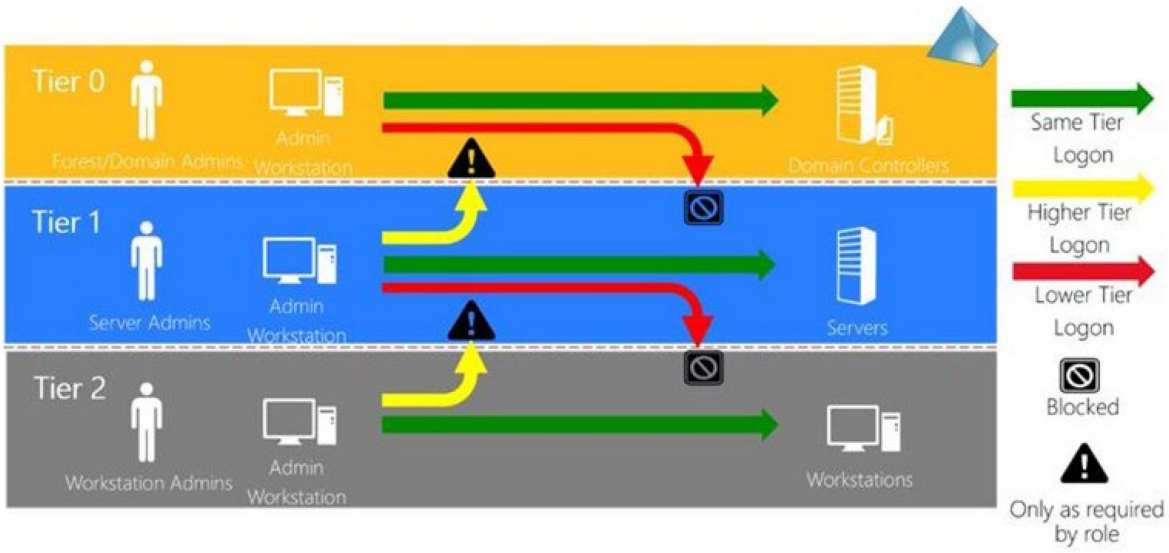

Abbildung 2: Schichtentrennung Soll – Logon (Quelle: Microsoft)

In Abbildung 3 wird von Control gesprochen, was in unserem Kontext privilegierte Zugriffe sind, um zu steuern, zu konfigurieren resp. zu administrieren oder dementsprechend zu kontrollieren, dies jedoch, ohne sich an den Systemen interaktiv anzumelden.

Prinzipiell passiert die Control innerhalb des jeweiligen Tiers (Same Tier Control, grüner Pfeil). Controls aus einer Schicht auf Systeme übergeordneter Schichten sind nicht zulässig. (Bsp. von Schicht 1 nach Schicht 0; Higher Tier Control; roter Pfeil).

Controls aus einer Schicht auf Systeme unterliegender Schichten sind nur mit eingeschränkten und absolut notwendigen Rechten zulässig (Lower Tier Control; gelber Pfeil).

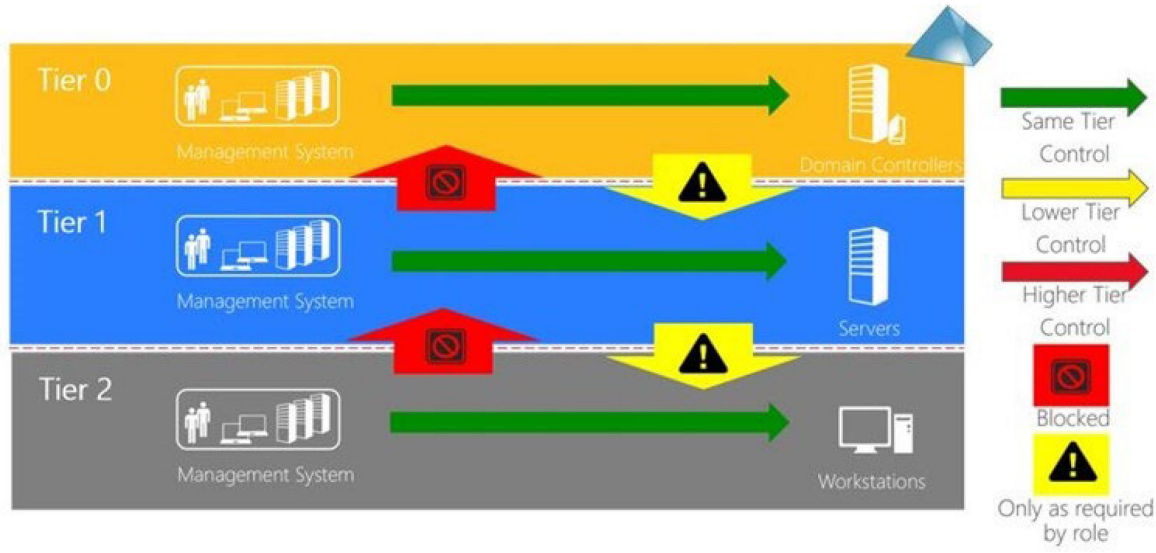

Abbildung 3: Schichtentrennung Soll – Control (Quelle: Microsoft)

Detaillierung der Bilder (Quelle von Bildern und Text: Microsoft)

• Tier 0-Accounts administrieren die Tier 0-Systeme und können sich interaktiv nur an Tier 0-Systemen anmelden • Tier 0-Accounts können Assets in jedem Tier verwalten.
• Tier 1-Accounts administrieren die Tier 1-Systeme und können sich interaktiv nur an Tier 1-Systemen anmelden • Tier 1-Accounts können auf Assets auf Tier 0 lesend zugreifen („via network logon type“) • Tier 1-Accounts können Assets in Tier 1 und 2 verwalten
• Tier 2 Accounts administrieren die Tier 2-Systeme und können sich nur an Tier 2-Systemen anmelden • Tier 2-Accounts können auf Dienste in allen Tiers zugreifen („via network logon type“) • Tier 2-Accounts können Assets in Tier 2 kontrollieren

Tabelle 2: Erklärung der unterschiedlichen Berechtigungen des Tier-Modells

Benutzerzugriffe auf Tier 1 und Tier 0 Services
Abbildung 4 zeigt auf, dass innerhalb von Tier 1 und Tier 0 Systeme, Dienste, Funktionen und Services für Endbenutzer (User) bereitgestellt werden.

In diesem Zusammenhang ist wichtig zu verstehen, dass sowohl Bundesinterne wie auch Bundesexterne bis hin zu Bürgern Zugang zu Tier 1-Systemen, -Diensten, -Funktionen und -Services, jeweils im Kontext eines Benutzers (nicht Administrators; nicht mit privilegierten Accounts), erhalten können. Damit passiert auf dieser Ebene somit kein Login oder Control auf Tier 1- und Tier 0-Systeme.

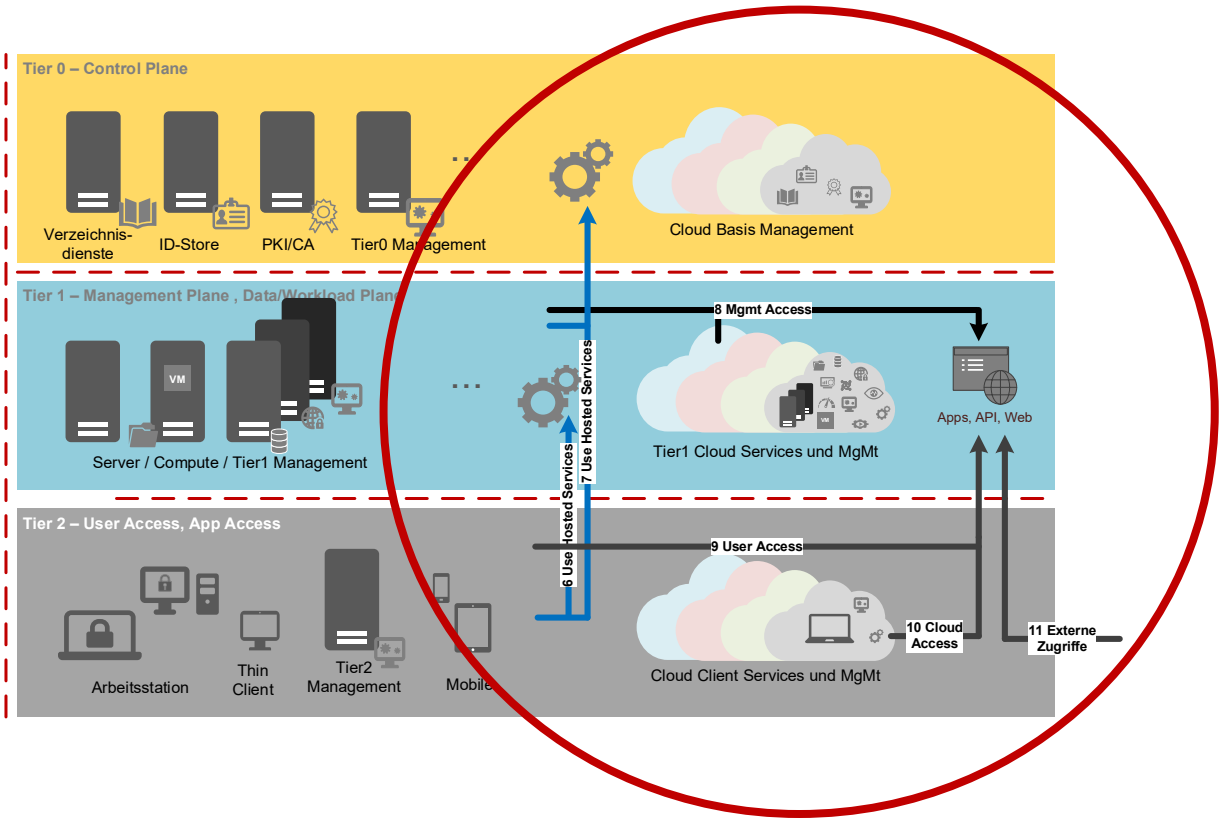

Abbildung 4: Schichtentrennung Soll - User Access (Quelle: eigene Grafik)

4.3 Account-Kategorien und Typen

Die nachfolgende Tabelle zeigt die Definition der verschiedenen Account-Kategorien und –Typen.

	Account Kategorie/Typ	Ausprägung
1	Lokaler System-Account	• Local System Accounts auf Schicht X-Systemen/Hardware/Device/Firmware • Operatoren-Accounts, die auf Schicht X-Systemen laufen • Service Accounts, die auf Schicht X-Systemen laufen
2	Verzeichnisdienst-Account	• Verzeichnisdienst-Administratoren auf Schicht X-Verzeichnisse • Verzeichnisdienst-Operatoren auf Schicht X-Verzeichnisse • Verzeichnisdienst-Service Accounts auf Schicht X-Verzeichnisse
3	Applikations-Account	• Privilegierte Applikations-Accounts, die auf Schicht X-Systemen/Applikationen laufen
4	Notfall-Account	• BreakGlass-Accounts

Tabelle 3: Definition der verschiedenen Account-Kategorien und -Typen

4.4 Systeme und Accounts im Schichtenmodell

Nachfolgende Tabelle zeigt die Definition der privilegierten Konten und der IKT-Systeme sowie deren Zuordnung in die drei Schichten im Schichten-Modell der Bundesverwaltung.

Jeder Account-Typ gemäss Tabelle 2 kann in allen Schichten/Tiers vorkommen.

Schicht	System/Device	Account/Konto	Prinzipien
PA	PAM	PAM-Administrator	Schicht PA "Privileged Access" beinhaltet PAM-Systeme/Komponenten.
0	• Domain Controller • PKI/CA • IAM (MIM/IDM/CIS ...) • Management für Schicht PA • Management für Schicht 0 • Hypervisor für Schicht 0 • Public Cloud	• Active Directory Domain Administrator • Certificate Authority/PKI Administrator • IAM Administrator • Management Administrator Hypervisor Administrator • Cloud-Administratorenrollen	Schicht 0 beinhaltet Identitäten führende Systeme mit ihren Diensten, Funktionen und Anwendungen sowie deren Management-Systeme und hochprivilegierte Schlüsselrollen der Cloud, die direkte oder indirekte Kontrolle über die Cloud-Infrastruktur haben.
1	• Applikations-Server (SAP ...) • Netzwerk-Infrastruktur (Firewall, RAS/VPN, SDN, Switches, …) • Hypervisor für Schicht 1 & 2 • Management für Schicht 1 & 2 nicht interaktiv • Haustechnik (Domotik) • Backend Systeme • Public Cloud	• Server-Administratoren • Server-Operatoren • Netzwerk-Administratoren • Hypervisor Administrator • Management Administratoren • Management Operatoren • Haustechnik-Administrator • Backend System Administrator • Cloud-Rollen	Server-Systeme mit ihren Diensten, Funktionen, Anwendungen und auch Managementsystemen
2	• APS/BA Clients • Hypervisor für Schicht 2 • Management für Schicht 2 • Drucker • Public Cloud	• APS-Administratoren • APS-Operatoren • Hypervisor-Administrator • Management-Administrator • Drucker-Administrator • Cloud-Rollen	Client-Systeme (Endbenutzergeräte)

Tabelle 4: Zuordnung der Systeme/Konten/Prinzipien zu den entsprechenden Schichten

Können Systeme oder Konten aufgrund dieser Liste nicht eindeutig zugewiesen werden, müssen diese mit der Sicherheitsorganisation der Verwaltungseinheit den Schichten (Tiers) zugeordnet werden.

5 Schlussbestimmungen

5.1 Aufhebung bisheriger Vorgaben

1. Keine Vorversionen

5.2 Übergangsbestimmungen

1. Für die Umsetzung des Tier-Modells gelten die Übergangsbestimmungen des Hauptdokuments.
2. Komponenten und Systeme des SD BA müssen im Rahmen des Programms MCT in die richtigen Tiers platziert werden.

5.3 Einhaltung

1. Die Departemente und die Bundeskanzlei sind gemäss VDTI für die Umsetzung dieser Weisungen in ihrem Zuständigkeitsbereich verantwortlich.

5.4 Überprüfung

1. Die BK(DTI) überprüft die Aktualität und Zweckmässigkeit dieser IKT-Vorgabe spätestens vier Jahre nach der Inkraftsetzung der vorliegenden Version.

5.5 Inkrafttreten

1. Diese Beilage zur IKT-Vorgabe tritt mit der Hauptversion in Kraft.

Anhänge

A. Änderungen gegenüber Vorversion

Versions-nummer	Datum	Autor	Änderungen
Entwurf 0.1	14.09.2021	Stefan Mueller (BIT), Bruno Schöb (BK), David Augustin (BK)	Initialversion. Vom Fachausschuss MCT akzeptiert.
Version 0.9	09.12.2021	Michael Hanspach (BK)	Freigabe zum Gebrauch im Projekt MCT.
Version 1.0	01.02.2023	David Augustin (BK) Bruno Schöb (BK)	Überarbeitung der Massnahmen.

B. Referenzen

ID	Referenz[3]
CyRV	Cyberrisikenverordnung, CyRV vom 27. Mai 2020 (Stand am 1. Januar 2021); SR 120.73
[ISchV]	Verordnung vom 4. Juli 2007 (Stand am 1. Januar 2018) über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV; SR 510.411)
[RFC 2119]	Request for Comments: 2119 (PCB14), The Internet Engineering Task Force (IETF)
RVOV	Regierungs- und Verwaltungsorganisationsverordnung (RVOV) vom 25. November 1998 (Stand am 1. Juni 2013); SR 172.010.1
[SB000]	SB000 – IKT-Strategie des Bundes 2020.2023 vom 3. April 2020
[VDTI]	Verordnung über die digitale Transformation und die Informatik, VDTI; vom 25. November 2020, SR 172.010.58

C. Abkürzungen

Kürzel	Bedeutung

[3] Erlasse auf Bundesstufe werden gemäss der «Systematischen Rechtssammlung» referenziert. Bei einer referenzierten Weisung zur Bundesinformatik wird die zum Ausgabedatum dieser Beilage gültige Version angegeben.