Mandantenübergreifende Konsolidierung polizeilicher IT- Verfahren bei Dienstleistern

Informationen zum Dokument	
Dokumentenart:	Standard KomSi
Dokumententitel:	Konsolidierung polizeilicher Verfahren
Dokumentennummer:	V1.0
Verantwortlicher:	KomSi – UAG-Technik
Dateiname:	180806 Mandantenübergreifende Konsolidierung polizeilicher IT- Verfahren bei Dienstleistern_UAG-Technik_V1.0.docx
Seitenzahl:	
Vertraulichkeitsstufe:	ohne
Freigabe am:	
Freigegeben durch:	

Änderungsnachweis				
Versions-nummer	Bearbeitungs-status	Datum	Bearbeiter	Änderung/Bemerkung
0.1-00	Initialversion	26.09.2017	UAG-Technik	
0.1-01	1. Arbeitsversion		UAG Technik	
0.8-01	Entwurf an KomSi	12.06.2018	UAG Technik	
1.0-01	Vorlage UA IuK	06.08.2018	UAG Technik	

Ergänzende Dokumente/Mitgeltende Unterlagen*			
Dokumentennummer	Titel des Dokuments	Version / Datum	Verantwortlicher
ohne	Verfahrensstandard für Anforderungen an Dienstleister vom 17.02.2016	1.0 / 17.02.2016	KomSi (UAG-Technik)

*In der Tabelle sind Dokumente einzutragen, die für dieses Dokument Gültigkeit besitzen, die aber im Dokument nicht explizit genannt werden, sowie alle Dokumente, auf die im nachfolgenden Dokument explizit verwiesen wird

Inhaltsverzeichnis

Einleitung 5
Auftrag 6
Ziel 6
Abgrenzung 6
Kapitel 1: Grundaussagen 7
1.1 Begrifflichkeiten 7
1.2 Kernaussagen 10
1.2.1 Allgemein 10
1.2.2 Dienstleister 10
1.2.3 Schutzzonen 10
1.3 Nachweisführung einer sicheren Trennung sowie Überprüfung 14
1.4 Vereinbarungen mit Dienstleistern 14
Kapitel 2: Mindestanforderung Virtualisierung 16
2.1 Vorgehensweise Klassische Virtualisierung 16
2.2 Konzeptioneller Aufbau der Ebenen 17
2.3 Mindestanforderungen 18
Anlage 1: Ebene 1: Client-Zugriffsebene (User) 19
Anlage 2: Ebene 2: Sicherheitsinfrastruktur (Perimeterschutz) 20
Anlage 3: Ebene 3: Anwendungen und Datenhaltung 21
Anlage 4: Ebene 4: IT-Infrastruktur 24
Anlage 5: Erweiterte Anforderungen an die Administration der Ebenen 1-4 25
Anlage 6: Beispiele einer Isolierung 27
Anlage 7: Erläuterungen zur Referenzarchitektur an Hand von Beispielen 29
Kapitel 3: Software-Defined-DataCenter SDDC 34
3.1 Erweiterte Begrifflichkeiten 36
3.2 Erweiterte Kernaussagen im Zusammenhang mit SDDC 38
3.3 Vorgehensweise Software Defined Datacenter - SDDC 40
3.4 Konzeptioneller Aufbau der Ebenen 41
3.5 Management im SDDC 43
3.6 Prozesse und Rollen im SDDC 45
3.7 Mindestanforderungen 47
Anlage 8: Ebene 1: Client – Zugriffsebene - SDDC 48
Anlage 9: Ebene 2: Sicherheitsinfrastruktur (Perimeterschutz) - SDDC 49
Anlage 10: Ebene 3: Anwendungen und Datenhaltung (Service / App) - SDDC 50
Anlage 11: Ebene 4: IT-Infrastruktur - SDDC 52
Anlage 12: Erweiterte Anforderungen an die Administration der Ebenen 1-4 - SDDC 53
Anlage 13: Erläuterungen zur Referenzarchitektur an Hand von Beispielen - SDDC 54

ABBILDUNGSVERZEICHNIS

ABBILDUNG 1: EBENE 1 - CLIENTZUGRIFF 7
ABBILDUNG 2: EBENE 2 - PERIMETEREBENE 8
ABBILDUNG 3: EBENE 3 - ANWENDUNG UND DATENHALTUNG 8
ABBILDUNG 4: EBENE 4 - INFRASTRUKTUR (BEISPIELHAFTE AUFZÄHLUNG) 9
ABBILDUNG 5: BEISPIEL POLIZEILICHE VERFAHREN OHNE EXTERNE ANBINDUNG 12
ABBILDUNG 6: BEISPIEL POLIZEILICHE VERFAHREN IM VERBUND OHNE EXTERNE ANBINDUNG 12
ABBILDUNG 7: BEISPIEL POLIZEILICHE VERFAHREN MIT SCHMUTZDATEN OHNE EXTERNE ANBINDUNG 13
ABBILDUNG 8: BEISPIEL POLIZEILICHE VERFAHREN UND ANBINDUNG AN INTERNET 14
ABBILDUNG 9: LOGISCHE DARSTELLUNG DER SCHUTZZONEN IM SINNE ISOLIERUNGSANFORDERUNGEN 17
ABBILDUNG 10: REFERENZARCHITEKTUR KLASSISCHE VIRTUALISIERUNG 18
ABBILDUNG 11: MANDANTENTRENNUNG PAAS - VARIANTE 1 22
ABBILDUNG 12: MANDANTENTRENNUNG PAAS - VARIANTE 2 23
ABBILDUNG 13: MANDANTENTRENNUNG IAAS 24
ABBILDUNG 14: KOMPONENTEN FÜR EINEN ADMINISTRATIVEN ZUGRIFF ÜBER DIE EBENEN HINWEG 26
ABBILDUNG 15: BEISPIEL MONITORING 27
ABBILDUNG 16: BEISPIEL DATENAUSTAUSCH 28
ABBILDUNG 17: DARSTELLUNG PRINZIPIELLER AUFBAU VON SCHUTZZONEN FÜR POLIZEILICHE VERFAHREN 29
ABBILDUNG 18: DARSTELLUNG PRINZIPIELLER AUFBAU SHARED APPLICATION 31
ABBILDUNG 19: DARSTELLUNG PRINZIPIELLER AUFBAU FAT-CLIENT-ANWENDUNG 32
ABBILDUNG 20: DARSTELLUNG PRINZIPIELLER AUFBAU SCHUTZZONEN SCHMUTZDATEN UND INTERNET 33
ABBILDUNG 21 DARSTELLUNG ENTWICKLUNG TRADITIONELLE IT HIN ZU CLOUD 34
ABBILDUNG 22: FIREWALL-PYRAMIDE 37
ABBILDUNG 23: PRINZIPIELLE DARSTELLUNG MANAGEMENT 42
ABBILDUNG 24:DARSTELLUNG PRINZIPIELLE MÖGLICHKEIT ZUR HÄRTUNG VON SERVICES 42
ABBILDUNG 25: BEISPIEL - LOGISCHER AUFBAU EINES MANAGEMENST IM SDDC 44
ABBILDUNG 26: BEISPIEL FÜR ROLLEN BEI NUTZUNG SDDC 45
ABBILDUNG 27: LOGISCHE ABBILDUNG EINER MÖGLICHEN SHARED APPLIKATION (FALL 3) AUF EBENE 4 54

Einleitung

Klassische Server-Installationen mit einer Anwendung je Server nutzen die vorhandenen Hardware-Ressourcen nur teilweise aus. Um die vorhandenen Kapazitäten effizient zu nutzen, werden IT-Systeme immer mehr virtualisiert, um flexibel auf Ressourcenbedarf und Anforderungen reagieren zu können.

Neben angestrebten finanziellen und personellen Einsparungen bieten Virtualisierungen sowie Cloud-Technologien auch Vorteile hinsichtlich der Skalierung von IT-Systemen. So lassen sich beispielsweise über das prognostizierte Maß hinausgehende Ressourcenbedarfe sehr dynamisch anpassen oder Hardwareausfällen können unproblematischer begegnet werden.

Dies führt gerade bei IT-Dienstleistern zu einem hohen Interesse, Kunden in virtualisierten, software definierten Rechenzentren (SDDC-software-defined-data-center) sowie cloudbasierten Umgebungen zu hosten, da sich, insbesondere in Rechenzentren, Ressourcen einsparen und IT-Systeme „kostengünstiger“ mit einem hohen Automatisierungsgrad betreiben lassen (Konsolidierung).

Die Situation der Haushalte und Personalzahlen innerhalb der Polizeien erfordern ebenfalls effizientere Auslastungen von IT-Systemen. Durch die Nutzung von Virtualisierungs-, SDDC- und Cloud-Techniken zur Konsolidierung von IT-Komponenten können jedoch zuvor durch „Hardware“ getrennte IT-Verbünde auch verschiedener Mandanten (siehe Definition 1.1) zusammengeführt werden. Dieser Umstand erfordert deshalb eine angepasste Bewertung der verwendeten und anzuwendenden Isolationsmechanismen sowohl aus Gründen der Informationssicherheit als auch des Datenschutzes.

Gleichzeitig zeigt sich eine Entwicklung hin zu wenigen großen IT-Dienstleistern, welche in ihren Rechenzentren für mehrere Mandanten Verfahren zentral bereitstellen. Hier zeigen sich die o.g. Synergieeffekte noch stärker, allerdings steigen damit auch die Risiken für den jeweils konsolidierten IT-Verbund. Dieser Umstand verstärkt die Forderung nach geeigneter Isolierung der Mandanten zusätzlich. Die Kommission IuK-Sicherheit setzte die „Unterarbeitsgruppe Virtualisierung/Technik“ ein, um die o.g. Problematik der Absicherung virtueller IT-Systeme im polizeilichen Umfeld, insbesondere bei IT-Konsolidierung, zu betrachten.

Mitglieder der „UAG Technik“ sind Vertreter BKA, (BSI), HB, HH, SH und SL; Sprecher der Arbeitsgruppe ist der Vertreter HB.

Das Dokument richtet sich in erster Linie an IT-Experten und IT-Sicherheitsbeauftragte.

Die Thematik der Virtualisierung, SDCC und Konsolidierung teilt sich auf in folgende Dokumente:

Kapitel 1:	0 – Mandantenübergreifende Konsolidierung polizeilicher Verfahren (Grundsatzpapier)
Kapitel 2:	1 - Mandantenübergreifende Konsolidierung polizeilicher Verfahren (Mindestanforderung Virtualisierung)
Kapitel 3:	2 - Mandantenübergreifende Konsolidierung polizeilicher Verfahren (Mindestanforderung an Software-Defined-DataCenter SDDC)
Anlage	Verfahrensstandard für Anforderungen an Dienstleister vom 17.02.2016

Auftrag

Folgende Themenschwerpunkte sollten hierbei im Hinblick auf die polizeiliche IT berücksichtigt werden:

- Virtualisierung von Anwendungen auf gleicher Hardware bei behörden- und länderübergreifender Nutzung (IT-Dienstleister ist für mehrere Mandanten zuständig),
- gemeinsame Nutzung aktiver Netzwerkkomponenten (Switche) durch polizeiliche und nichtpolizeiliche Mandanten mit unterschiedlichem Sicherheitsniveau,
- "Software Defined Networking (SDN)" als "Infrastructure as a Service (IaaS)",
- „Software Defined Data Center“ SDDC,
- Cloud-Computing,
- Fortschreibung des Dokumentes unter Einbeziehung technologischer Entwicklungen.

Die genannten Themenschwerpunkte werden unter nachfolgenden Mandantenkonstellationen betrachtet:

- Polizei – Polizei
- Dritte[1] – Polizei.

Dabei werden entstehende Risiken betrachtet u.a. durch Nutzung von

- Virtualisierten IT-Systemen auf gemeinsamer physikalischer Hardware,
- Services in einem SDDC,
- Private Cloud,
- Mandanteneigenen Anwendungen auf gemeinsamen physikalischen oder virtualisierten IT-Systemen (SDDC/Cloud),
- Mandantentrennung innerhalb der Anwendung auf einer Hardware oder einem virtualisierten IT-System (SDCC/Cloud),
- gemeinsame Netzwerkressourcen (physikalisch/virtuell, SDN),
- mandantenübergreifende Cloud-Infrastrukturen sowie,
- sich dynamisch ändernde IT-Umgebungen.

Ziel

Erstellung von produktunabhängigen Mindestanforderungen für die mandantenübergreifende Konsolidierung polizeilicher IT- Verfahren bei Dienstleistern.

Abgrenzung

Gesetzliche (u.a. Datenschutz; Verschlusssachenanweisung) und behördliche Vorgaben (z.B. Beschlüsse aus AKII; UA IuK) bleiben vom vorliegenden Dokument unberührt.

---

1 Dritte i.S. dieses Arbeitspapieres sind alle „Nicht-Polizeien“ (210. Sitzung AKII, 29.03.2007)

Kapitel 1: Grundaussagen

Das hier aufgeführte Grundsatzpapier stellt übergeordnete Rahmenbedingungen dar. Die nachfolgenden Kapitel präzisieren die Möglichkeiten der Konsolidierung in Abhängigkeit der eingesetzten Technik.

1.1 Begrifflichkeiten

Demilitarisierte Zone (DMZ)

Eine DMZ stellt eine Netzsegmentierung dar, die über eine Sicherheitskomponente ausgebildet wird.

Dienstleister (IT-Dienstleister)

Erbringt die IT-Dienstleistung/den IT-Service für einen oder mehrere Kunden.

Ebenen

Die Ebenen stellen die verschiedenen Bereiche eines Informationsverbundes dar, welche durch eine Virtualisierung und Konsolidierung betroffen sind. Die Ebenen sind dabei aufgeteilt in 4 Ebenen:

Ebene 1: Client-Zugriffsebene (User)

Ebene 1 stellt die Zugriffsebene dar, in der jeder Mandant eine eigene Client-Infrastruktur hat. Der Zugriff des Nutzers über den Client auf die Service erfolgt über die Anbindung an Ebene 2 (Perimeterebene). Bei der Polizei wären dies z.B. die in der CNP-UN stehenden Clients.

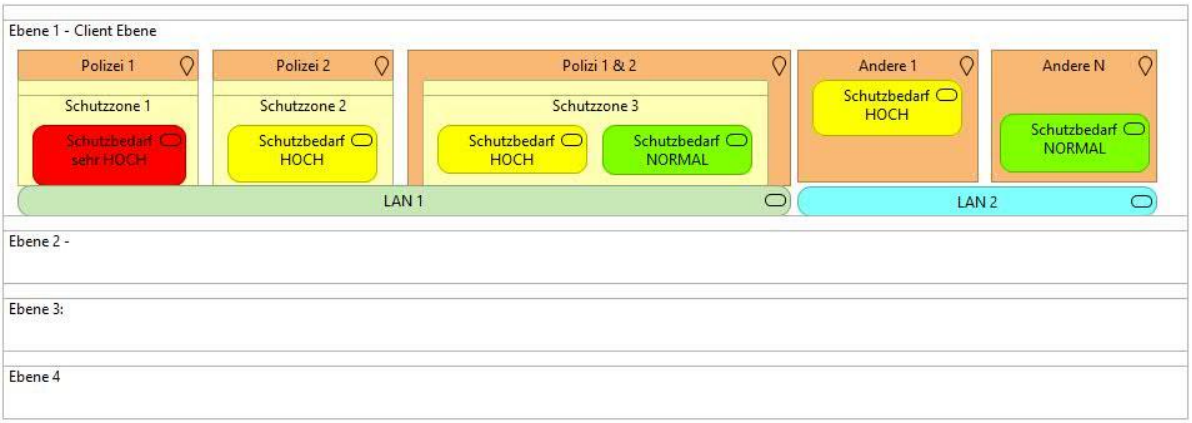

Abbildung 1: Ebene 1 - Clientzugriff

Ebene 2: Sicherheitsinfrastruktur (Perimeterschutz)

Diese Ebene bildet den klassischen Perimeterschutz und beinhaltet (aktive) Sicherheitskomponenten wie Paketfilter, ALG, XML-Gateways, API-Management, Proxys, Loadbalancer, IDS/IPS, Access-Gateways etc.

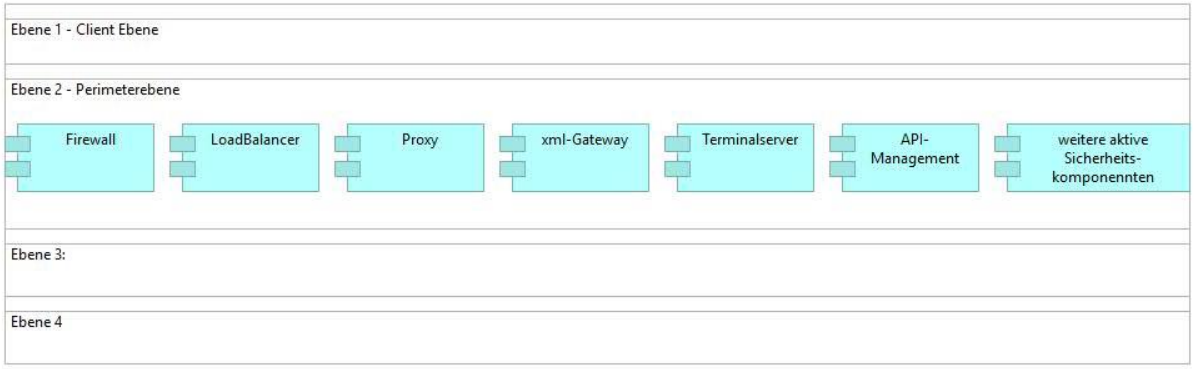

Abbildung 2: Ebene 2 - Perimeterebene

Ebene 3: Anwendungen und Datenhaltung

In Ebene 3 werden Dienste (Services) bereitgestellt. Diese werden in separaten Schutzzonen betrieben (siehe 1.1). In den Schutzzonen wiederum befinden sich jeweils eine oder mehrere Demilitarisierte Zonen (DMZ) bzw. Service-Schutz-Gruppen. Innerhalb der Schutzzonen können sich Applikations- und Web-Server, fachliche und infrastrukturelle Querschnittsdienste, Terminalserverinfrastrukturen sowie die Datenhaltung befinden. Eine gemeinsame mandantenübergreifende Nutzung von Schutzzonen ist grds. möglich (siehe Anlage 3: Ebene 3: Anwendungen und Datenhaltung). Die Kommunikation zwischen DMZen bzw. zwischen Service-Schutz-Gruppen untereinander erfolgt innerhalb einer Schutzzone über Paketfilter (s. Schutzzone 2). Im Zusammenhang mit Cloud-Techniken werden in dieser Ebene die Service „Infrastructure as a Service (IaaS)“, „Platform as a Service (PaaS)“ und „Software as a Service (SaaS)“ betrieben.

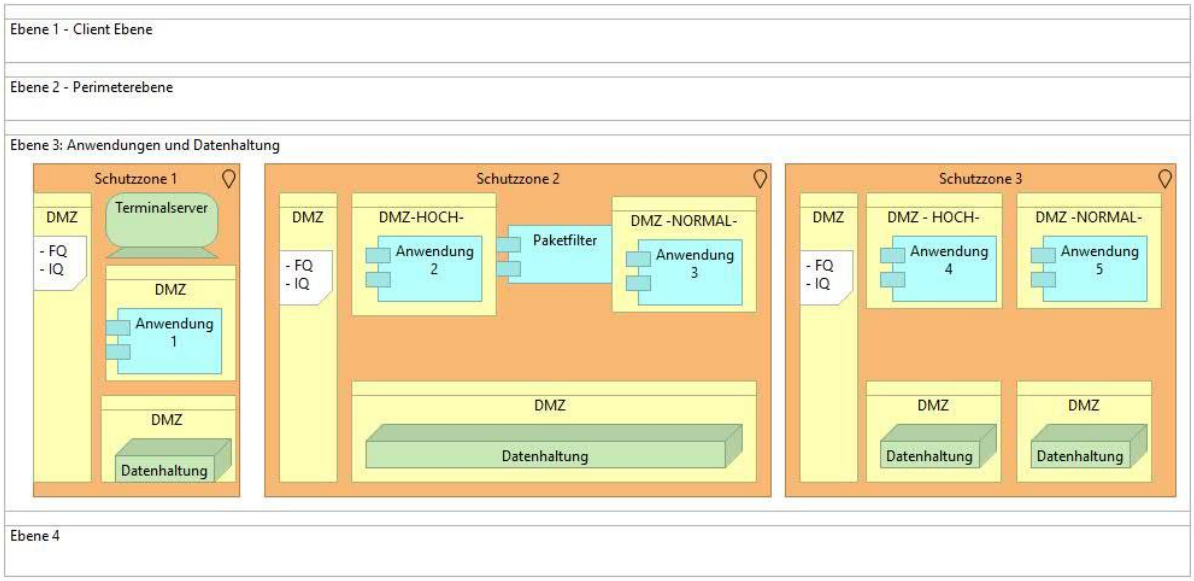

Abbildung 3: Ebene 3 - Anwendung und Datenhaltung

Ebene 4: IT-Infrastruktur

Diese Ebene beinhaltet die IT-Infrastrukturebene (Netze, Storage, Computenodes und weitere HW-Ressourcen) und stellt die Ressourcen für die Ebene 3 dar.

Abbildung 4: Ebene 4 - Infrastruktur (beispielhafte Aufzählung)

Mandant

Unter Mandant wird hier der jeweilige Kunde verstanden, wobei die Polizei hierbei ein Mandant darstellt. Mandant können sein die Polizei oder auch „Dritte“ (z.B. eine Bundes-/Landesbehörde, externes Unternehmen).

Schutzbedarf

Der Schutzbedarf beschreibt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist, zur Gewährung der Schutzziele/Grundwerte (Vertraulichkeit; Integrität; Verfügbarkeit) der Informationssicherheit. Darüber hinaus gewinnen aber auch Grundwerte, die sich aus dem Datenschutz heraus entwickeln, immer mehr an Bedeutung.

Schutzzone

Schutzzonen sind logisch zu bildende Gruppierungen von Geschäftsprozessen und der ihnen zugrundliegenden Daten, aufgrund der auf sie wirkenden oder von ihnen ausgehenden Risiken. Innerhalb der Schutzzone können Daten unterschiedlicher Schutzbedarfe verarbeitet werden. Diese werden entsprechend in DMZen bzw. Service-Schutz-Gruppen separiert.

Service-Schutz-Gruppen

Bei Einsatz von SDDC-Umgebungen werden mittels Service-Schutz-Gruppen die Service und Daten bezüglich der durchzuführenden Sicherheitsmechanismen zusammengefasst und klassifiziert.

1.2 Kernaussagen

1.2.1 Allgemein

- Umgebung(en) Dritter und Umgebung(en) Polizei sind mittels geeigneter Netzwerkseperationsmechanismen (z.B. physikalisch getrennte LANs oder vergleichbare Schutzmaßnahmen wie Hypervisor-Sicherheitsmechanismen, Verschlüsselung) an die Perimeter Ebene des Dienstleisters anzubinden.
- Der Zugriff von außen erfolgt über Paketfilter und zusätzliche aktive Sicherheitskomponenten (z.B. ALG).
- Eine mandantenübergreifende Konsolidierung unter Nutzung von Virtualisierungs- und software-definierten Techniken ist grundsätzlich möglich. Die Anforderung an die Stärke der Trennungsmechanismen für eine fachliche Konsolidierung zwischen Polizeien ist dabei geringer, als bei einer Konsolidierung über verschiedenste Mandanten („Dritte“) hinweg.
- Infrastruktur (Ebene 4) kann bei ausreichender Isolierung gemeinsam genutzt werden. Die Nutzung gemeinsamer Cluster zwischen Polizei(en) und Dritter ist nicht möglich. Die Kommunikation mit Dritten sowie nach „Außen“ erfolgt über die Perimeterebene (Ebene 2).
- Applikation und Datenhaltung werden über FW-Strukturen getrennt.

1.2.2 Dienstleister

- Bei Hosting durch einen zentralen Dienstleiter sind Umgebungen(en) Dritter von Umgebungen(en) der Polizei auf allen Ebenen sicher zu trennen.
- Hierbei trennen die Dienstleister polizeiliche Daten und Daten Dritter mittels eigener LAN oder vergleichbarer Schutzmaßnahmen und zusätzlicher aktiver Sicherheitskomponenten über die Perimeterebene oder bei Nutzung von Cloud-Technologien auch über software-defined-Sicherheitsmechanismen.
- Die Kommunikation zu Dritten ist über die Perimeter Ebene zu führen.

1.2.3 Schutzzonen

- Die sich aus bestimmten Bedrohungsszenarien (Risiken/Eintrittswahrscheinlichkeiten) heraus ergebenden Angriffe auf
    - Mandanten und/oder
    - Geschäftsprozesse und/oder
    - Kommunikationsbeziehungen

  können u.a. auch durch (Netz)Separierungen der Anwendung/Service per DMZ oder Service-Schutz-Gruppen minimiert werden.

- Die Einteilung in Schutzzonen und Service-Schutz-Gruppen richtet sich nach
    1. der Art der verarbeiteten Daten einerseits (polizeiliche Daten, interne Daten, Schmutzdaten, Daten von denen eine Gefährdung ausgeht, Daten unbekannter Quelle etc.),
    2. der Art der Kommunikationspartner (vertrauenswürdig /Polizei, nichtvertrauenswürdig /Dritte),
    3. dem Zugriffsweg, d.h. von wo aus greift der Partner auf die Daten zu (CNP, Behördennetz, Internet).

- Für polizeiliche Daten können sich u.a. folgende Schutzzonen per DMZen und Service-Schutz-Gruppen, Teile oder beliebige Kombinationen ergeben (siehe Beispiele):
  1. Interne polizeiliche Verfahren ohne externe Anbindung
  2. Verbund- und mandantenübergreifende polizeiliche Verfahren
  3. Verarbeitung von Schmutzdaten (z.B. Forensik, TKÜ) – potentiell schadcodebehaftete Daten
  4. Polizeiliche Services am Internet (z.B. Internetnahe Dienste, Internetrecherche, e-Gouvernement-Verfahren).

Die hier getroffene Reihenfolge gibt bereits die Vertrauenswürdigkeit der Schutzzonen und Service-Schutz-Gruppen und damit ein Ranking wieder.

Zur Bildung von Schutzzonen, über DMZen und Service-Schutz-Gruppen ausgeprägt, wird nie der Schutzbedarf einer Anwendung herangezogen, da der Schutzbedarf sich immer nur auf die in den Segmentierungen verarbeitenden Daten bezieht.

- Zusätzliche Schutzzonen und Service-Schutz-Gruppen können sich in Abhängigkeit erweiterter Aufgaben/Anforderungen ergeben.
- Gleichartig risikobehaftete Verfahren können gruppiert und innerhalb einer Schutzzone gemeinsam unter Beachtung eines geeigneten Sicherheitskontextes gebündelt und abgesichert werden. Dieses gilt auch für Verbundverfahren, die für mehrere Teilnehmer gemeinsam betrieben werden. In diesem Falle liegt das Erfordernis des Nachweises der Trennung im Sinne des Datenschutzes auch innerhalb des Verfahrens.
- Schutzzonen und Service-Schutz-Gruppen sind entsprechend der auf sie wirkenden oder von ihnen ausgehenden Risiken, über geeignete Separierungsmechanismen getrennt zu betreiben.
- Für die Verarbeitung von polizeilichen Daten sind grundsätzlich eigene Schutzzonen auf eigenen Ressourcen zu bilden.
- Eine Konsolidierung bzw. die Nutzung gemeinsamer Komponenten einer Schutzzone oder Service-Schutz-Gruppe ist über alle polizeilichen Daten möglich, unter Berücksichtigung einer ausreichenden Isolierung und der Nachweisführung sicherer Trennungsmechanismen (s. Pkt. 2.3).
- Über Service-Schutz-Gruppen können Geschäftsprozesse selektiver abgegrenzt werden.

Beispiele für Schutzzonen, Service-Schutz-Gruppen und jeweils mögliche Kombinationen:

1. Polizeiliche Daten/Verfahren ohne externe Anbindung
   - werden nur innerhalb des Teilnehmers im polizeilichen Informationsverbund zur Verfügung gestellt
   - sind keine Schmutzdaten (z.B. TKÜ, forensische Auswertung)
   - kein Zugriff von Dritten

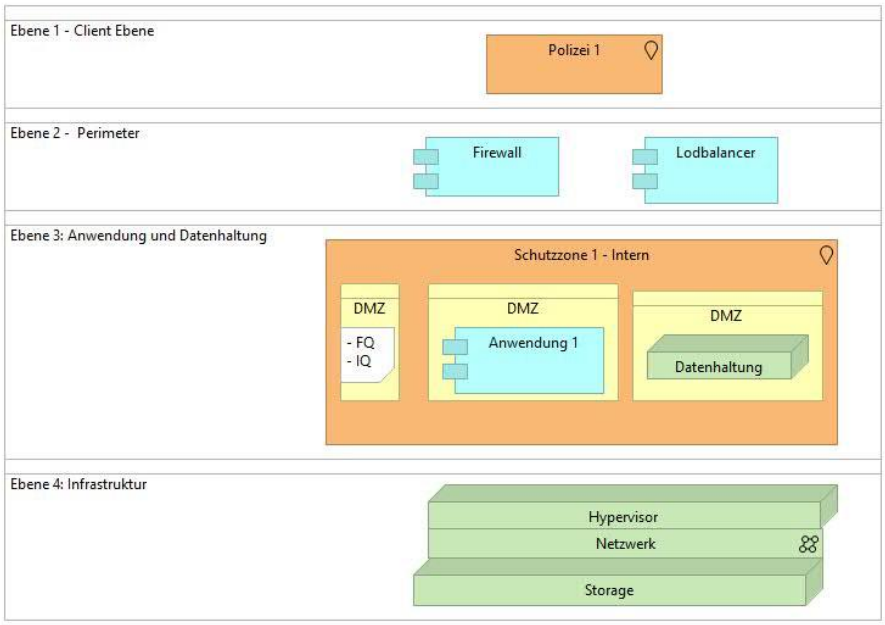

Abbildung 5: Beispiel polizeiliche Verfahren ohne externe Anbindung

2. Polizeiliche Daten/Verfahren sowie interne polizeiliche Verfahren ohne externe Anbindung
   - werden innerhalb des polizeilichen Informationsverbund zur Verfügung gestellt
   - sind keine Schmutzdaten (z.B. TKÜ, forensische Auswertung)
   - kein Zugriff von Dritten

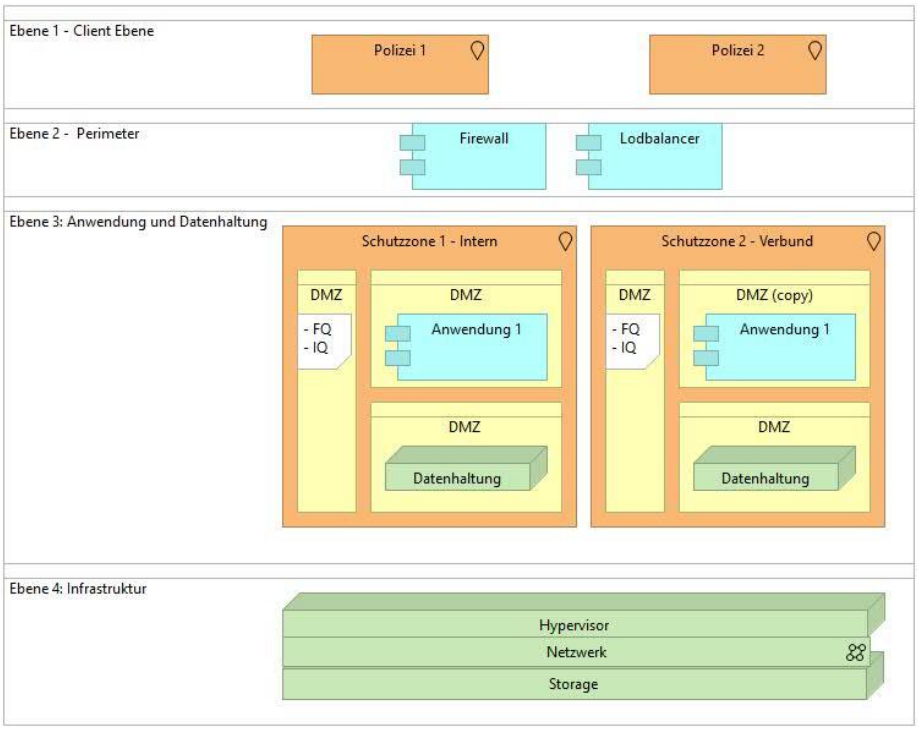

Abbildung 6: Beispiel polizeiliche Verfahren im Verbund ohne externe Anbindung

3. Polizeiliche Daten/Verfahren sowie Schmutzdatenanalyse ohne externe Anbindung
   - werden innerhalb des polizeilichen Informationsverbund zur Verfügung gestellt
   - sogenannte Schmutzdaten werden verarbeitet (z.B. TKÜ, forensische Auswertung)
   - kein Zugriff von Dritten

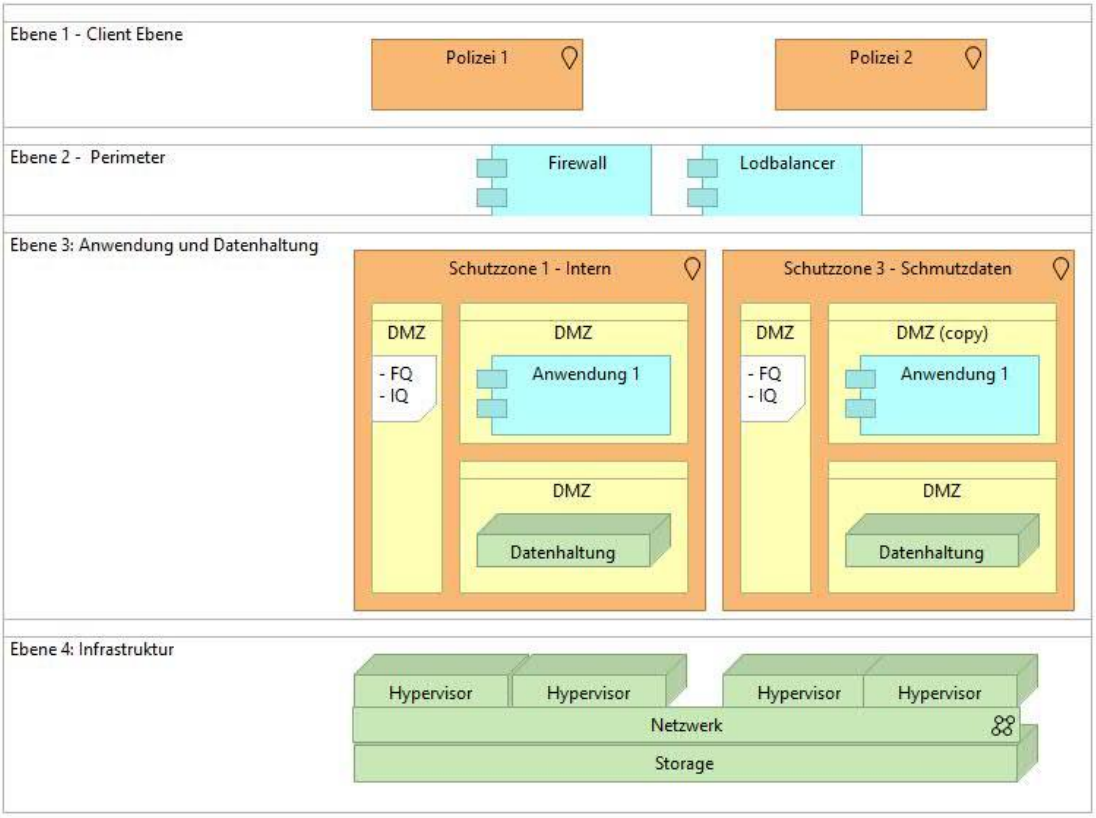

Abbildung 7: Beispiel polizeiliche Verfahren mit Schmutzdaten ohne externe Anbindung

4. Polizeiliche Daten/Verfahren mit Anbindung Internet
   - Ermittlungstätigkeiten am Internet
   - werden über Internet ausgetauscht
   - Zugriff von Dritten

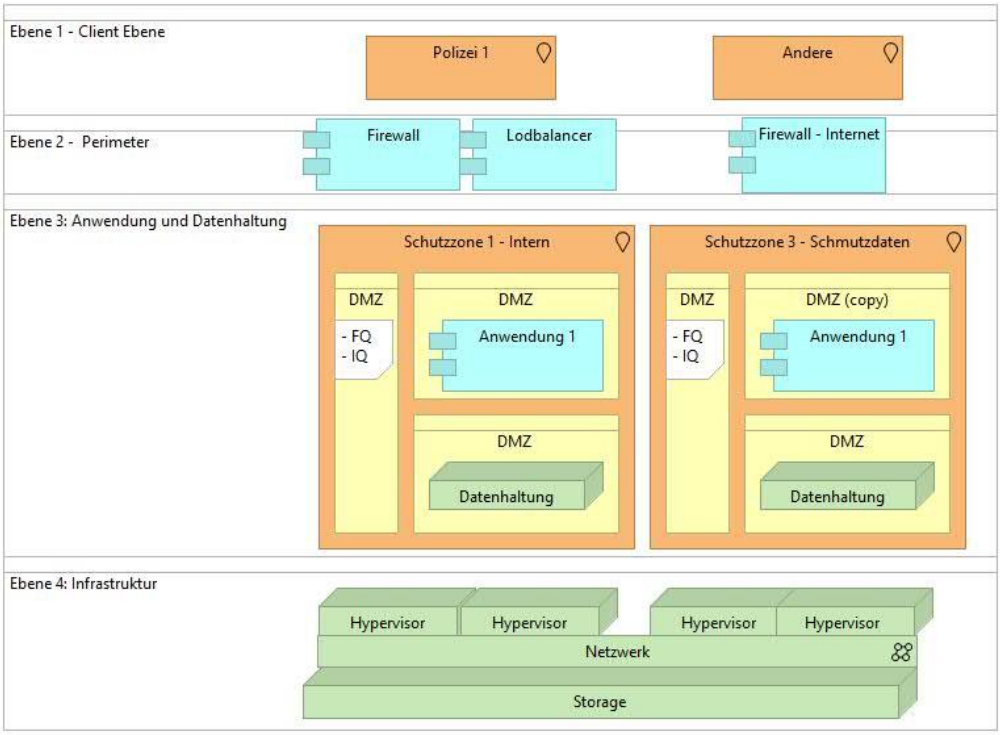

Abbildung 8: Beispiel polizeiliche Verfahren und Anbindung an Internet

1.3 Nachweisführung einer sicheren Trennung sowie Überprüfung

Es erfolgt eine Isolierung der polizeilichen Daten untereinander sowie gegenüber Daten Dritter. In den Anlagen zu dem vorliegenden Dokument finden sich oftmals Aussagen, dass neben einer physikalischen Trennung auch eine „vergleichbare Isolierung“ umgesetzt werden kann. In diesem Fall ist die Gleichwertigkeit folgendermaßen nachzuweisen:

1. Vor Inbetriebnahme muss ein Sicherheitskonzept nach BSI Standard 200-1 bzw. 200-2 abgestimmt vorliegen, das infrastrukturelle und verfahrensspezifische Maßnahmen sowie Aussagen über die in diesem Dokument beschriebenen Mindestanforderungen trifft.
2. Bereits bestehende Sicherheitskonzepte des Dienstleisters ersetzen das unter 1. geforderte Sicherheitskonzept nicht, können aber einfließen, um die Maßnahmenumsetzung in bestimmten Schichten nachzuweisen (bspw. Schicht 1 der Grundschutzkataloge). Auch die Vorlage eines Auditberichtes kann helfen, die Erstellung eines oben geforderten Sicherheitskonzeptes zu vereinfachen und ein angemessenes Sicherheitsniveau nachzuweisen.
3. Es ist eine Risikoanalyse nach BSI Standard 200-3 durchzuführen, in welcher die Wirksamkeit der Trennungsmechanismen dargestellt wird. Verbundübergreifende Risiken sind gesondert auszuweisen.
4. Der Auftraggeber prüft das Sicherheitskonzept vor Inbetriebnahme und stimmt verbleibende verbundübergreifende Risiken nach einem durch die KomSi festgelegten Prozess ab.

1.4 Vereinbarungen mit Dienstleistern

Mit dem externen Dienstleister sind Regelungen zu folgenden Punkte zu treffen.

- Abschluss von SLAs; Vereinbarung von Reaktionszeiten
- Incident Management
- Regelungen der Behandlung von Sicherheitsvorfällen beim Dienstleister
- Mandantenfähiges technisches, fachliches, sicherheitstechnisches Monitoring mit Auswertemöglichkeit des Kunden und Anbindung an CERT inkl. Revisionsmöglichkeit.

- Vor Wirkbetriebsaufnahme müssen der Dienstleister Sicherheits- und Betriebskonzepte zur Prüfung dem Kunden vorlegen.
- Möglichkeit zur Durchführung proaktiver IS-Revisionen: Audits durch den Kunden, durch andere Polizeien oder BSI.
- Analoge Umsetzung der in den nachfolgenden Bausteinen enthaltenen Empfehlungen: Baustein Cloud-Nutzung, Speicherlösung/Cloud-Storage, Cloud-Management, Outsourcing, Webanwendungen, Web-Services.
- Umgang mit Informationen, Vereinbarung zur Geheimhaltung, Informationssicherheit, Datenschutz, Sicherheitsüberprüfung.
- Protokollierung, Umfang der Protokollierung, sichere Protokollierung, mandantenübergreifende Protokollierung. Einsicht in technische, fachliche und sicherheitsrelevante Protokolle.
- Fernwartungszugriffe von externen Firmen auf polizeiliche Umgebungen, betrieben durch Kunde oder Dienstleister, müssen vertraglich geregelt werden.
- Konfigurationsdaten mit personenbezogenen oder sensiblen Inhalten, die Rückschluss auf die Polizei zulassen, dürfen nur auf vertraglicher Grundlage und je nach Einstufung an entsprechend verpflichtete Supportfirmen herausgegeben werden, wenn keine andere Möglichkeit der Problembehebung / Störungsbeseitigung gegeben ist oder ansonsten unmöglich wäre.
- Löschen bzw. sichere Vernichtung von Speichermedien (defekte oder auszutauschende Speichermedien etc.) mit Echtdaten (siehe BSI-TL 03420 und GS-Baustein B1.15 (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01015.html)).

Es gilt die Anlage: „Verfahrensstandard für Anforderungen an Dienstleister vom 17.02.2016“.

Kapitel 2: Mindestanforderung Virtualisierung

Nachdem in „Kapitel 1 Grundsatzpapier“ die grundlegenden Begrifflichkeiten dargestellt und Kernaussagen getroffen werden, baut Kapitel 2 inhaltlich darauf auf und betrachtet virtualisierte Umgebungen außerhalb Software-Defined-DataCenter (SDDC).

Die hier dargestellten Inhalte entsprechen dem vom UA IuK verabschiedeten Dokument „Mindestanforderungen an eine mandantenübergreifende Virtualisierung polizeilicher Verfahren“ aus 2016. Lediglich die übergreifenden Aspekte, die unabhängig der Technologien Gültigkeit haben, sind im übergeordneten Dokument (Grundsatzpapier) aufgenommen worden.

2.1 Vorgehensweise Klassische Virtualisierung

- Festlegung der Schutzzone(n).
- Ranking der Schutzzonen basierend auf den Bedrohungs- und Gefährdungsszenarien.
  Aus dem Ranking der Schutzzonen ergibt sich die Vorgabe des initialen Verbindungsaufbaus. Die Kommunikation zwischen den Schutzzonen erfolgt grundsätzlich aus der „höherwertigeren Schutzzone (vertrauenswürdiger)“ auf eine „niedrigere Schutzzone (weniger vertrauenswürdig)“ oder zwischen gleichwertigen Schutzzonen bidirektional.
- Administration und infrastrukturelle Querschnittsdienste sind von Daten zu trennen.
- Die jeweilige Infrastruktur innerhalb einer Ebene wird per Hardware oder Hypervisor zur Verfügung gestellt.
- Für jeden Mandanten werden pro Schutzzone eigene infrastrukturelle Querschnittsdienste eingerichtet. Der Nutzung von mandantenübergreifenden infrastrukturellen Querschnitts-diensten kann zugestimmt werden, wenn dies entsprechend begründet beantragt wird. Hierfür ist der Nachweis einer sicheren Isolierung (fachlich, administrativ und infrastrukturell) der Mandanten durch den Dienstleister zu erbringen.

2.2 Konzeptioneller Aufbau der Ebenen

Die Abbildung 9 stellt die Ebenen 1-4 mit verschiedenen Komponenten beispielhaft dar. Die Ebenen beschreiben eine Sicht vom User (Client-Ebene 1) bis zum infrastrukturellen Rechenzentrum (Ebene 4) - vertikale Sicht „Nord-Süd-Kommunikation“.

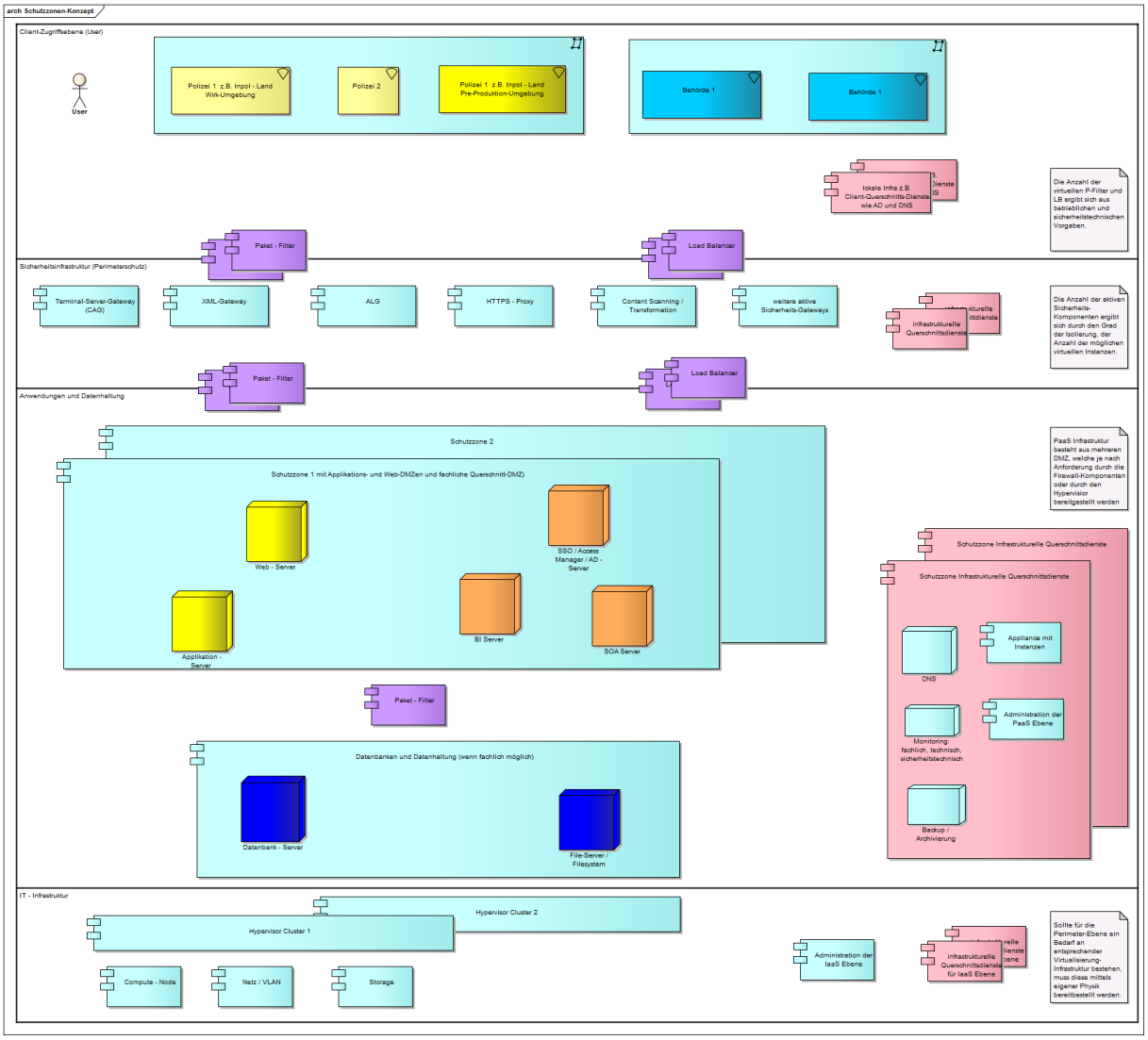

Abbildung 9: Logische Darstellung der Schutzzonen im Sinne Isolierungsanforderungen

Abbildung 10 zeigt aus Sicht der UAG eine Referenzarchitektur für die klassische Virtualisierung, wie sie nun im Folgenden in den Ebenen 1-4 näher erläutert wird (siehe auch Anlagen 1-4).

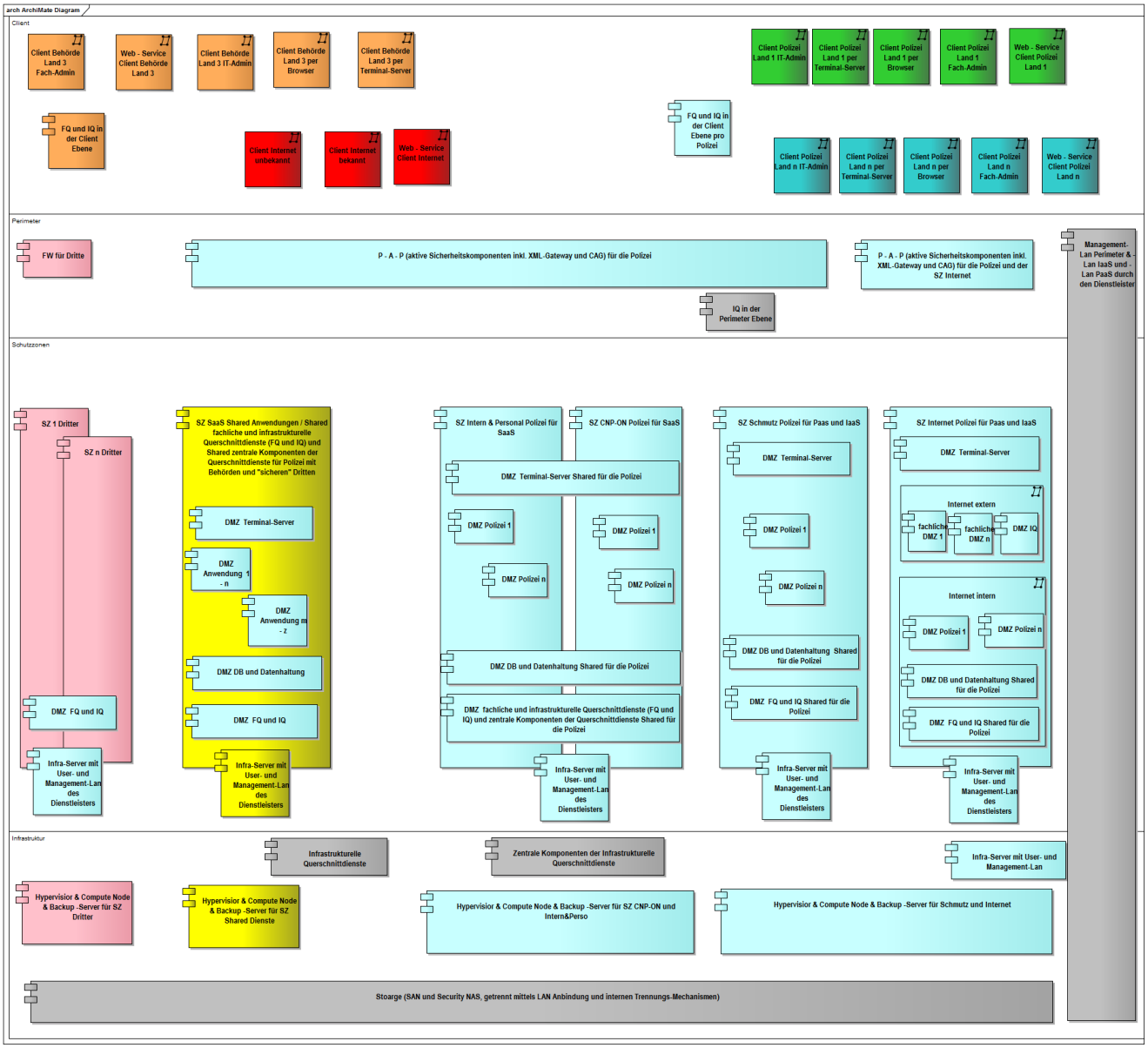

Abbildung 10: Referenzarchitektur klassische Virtualisierung

2.3 Mindestanforderungen

Die Mindestanforderungen an die unterschiedlichen Ebenen und Szenarien werden in

- Anlage 1: Ebene 1: Client-Zugriffsebene (User)
- Anlage 2: Ebene 2: Sicherheitsinfrastruktur (Perimeterschutz) Virtualisierung
- Anlage 3: Ebene 3: Anwendungen und Datenhaltung
- Anlage 4: Ebene 4: IT-Infrastruktur
- Anlage 5: Erweiterte Anforderungen an die Administration der Ebenen 1-4
- Anlage 6: Beispiele für eine Isolierung
- Anlage 7: Erläuterungen zur Referenzarchitektur an Hand von Beispielen

beschrieben. Dabei werden zunächst die Gefährdungen aufgeführt, welche bei mandanten-übergreifender Virtualisierung vorhanden sein können. Anschließend werden die umzusetzenden Maßnahmen aufgeführt.

Anlage 1: Ebene 1: Client-Zugriffsebene (User)

Zunächst werden die Gefährdungen der Ebene 1 beschrieben, die durch eine Konsolidierung entstehen können. Darauf aufbauend werden die umzusetzenden Maßnahmen aufgeführt.

Gefährdungen

- Keine Gewährleistung eines homogenen Sicherheitsniveaus über alle Mandanten, da Gremienbeschlüsse des AK II – Innere Sicherheit- nur innerhalb des polizeilichen Informationsverbundes bindend und durchsetzbar sind. Somit ist ein Gefälle beim Sicherheitsniveau von Polizeien zu Dritten möglich.
- Infektion der Clients durch Verwendung von Wechselmedien über offene Schnittstellen am Client.
- Zugriff der Clients auf unsichere Netze.
- Keine Überprüfung des Sicherheitsniveaus möglich.
- Kompromittierung durch eine Kopplung der Clients von mehreren Mandanten durch eine zentrale Administration dieser Clients.
- Kompromittierung durch eine Kopplung der Clients von mehreren Mandanten durch gemeinsame Nutzung (Konsolidierung) von fachlichen und infrastrukturellen Querschnittsdiensten.

Maßnahmen

- Pro Polizei-Client-Umgebung sind eigene Client-Querschnittsdienste wie AD/DNS usw. einzusetzen
    - Ausnahme:
      Eine Abweichung ist möglich, wenn der Dienstleister eine anderweitige sichere Trennung der Mandanten nachweisen kann (siehe 1.3).
- Client-Infrastruktur, die zentral gehostet wird, wird in der Ebene 3 (Anlage 3) betrachtet.
- Die fachliche Nutzung der Clients als User, Fachadministrator oder IT-Administrator in den unterschiedlichen Ebenen muss durch geeignete Maßnahmen abgesichert werden.

Anlage 2: Ebene 2: Sicherheitsinfrastruktur (Perimeterschutz)

Gefährdungen

- Kompromittierung durch fehlenden Trennungsmechanismus.
- Fehlkonfiguration der Sicherheitskomponenten beeinträchtigt alle Mandanten.
- Ausfall der Sicherheitskomponenten (Hardware) beeinträchtigt alle Mandanten.
- Kopplung der Mandanten durch konzeptionelle Schwächen im Trennungsmechanismus.
- Fehler in der Komponente die die logische Trennung durchführt.
- Kompromittierung durch eine Kopplung der Sicherheitskomponenten von mehreren Mandanten durch gemeinsame Nutzung (Konsolidierung) von fachlichen und infrastrukturellen Querschnittsdiensten.
- Sicherheitsinfrastruktur ist nicht hinreichend vor unbefugten Zugriff geschützt.

Maßnahmen

- Die Trennung der einzelnen Sicherheitskomponenten von Polizeien zu Dritten erfolgt durch eine physikalische Trennung oder einer vergleichbaren Isolierung (fachlich, administrativ und infrastrukturell).
- Für den Betrieb der Komponenten auf Hypervisor-Infrastruktur wird eine von den anderen Infrastrukturen getrennte, d.h. eigene Hypervisor-Infrastruktur für Ebene 2 benötigt.
- Umgebung(en) Dritter und Umgebung(en) Polizei sind getrennt über eigene LANs oder vergleichbare Schutzmaßnahmen an die Infrastruktur des Dienstleisters anzubinden.

Anlage 3: Ebene 3: Anwendungen und Datenhaltung

Gefährdungen

- Kompromittieren durch fehlenden Trennungsmechanismus.
- Fehlkonfiguration der Anwendungs- und Datenhaltungskomponenten beeinträchtigt alle Mandanten.
- Ausfall der Anwendungs- und Datenhaltungskomponenten (Hardware) beeinträchtigt alle Mandanten.
- Kopplung der Mandanten durch konzeptionelle Schwächen im Trennungsmechanismus.
- Fehler in der Komponente, die die logische Trennung durchführt.
- Kompromittieren durch eine Kopplung der Anwendungs- und Datenhaltungskomponenten von mehreren Mandanten durch eine zentrale Administration der Anwendungs- und Datenhaltungskomponenten.
- Kompromittieren durch eine Kopplung der Anwendungs- und Datenhaltungskomponenten von mehreren Mandanten durch gemeinsame Nutzung (Konsolidierung) von fachlichen und infrastrukturellen Querschnittsdiensten.
- Diebstahl oder Verfälschung von Nutzdaten.
- Nicht den gesetzlichen Vorgaben entsprechendes Löschen von Nutzdaten.

Maßnahmen

Unter dem Begriff fachliche Querschnittsdienste werden u.a. Job-Scheduling und File-Transfer-SW, SOA-, BI-, SSO-Dienste gebündelt. Diese zeichnen sich durch eine hohe Anforderung an eine Isolierung der Fachadministration und der Mandanten-Daten innerhalb der Applikation aus.

Schutzzone / Schutzzonen untereinander

- Schutzzonen werden über PAP-Strukturen (Paketfilter + aktive Sicherheitskomponenten + Paketfilter) abgebildet.
- Der Zugriff der Clients auf Schutzzonen sowie die Kommunikation zwischen Schutzzonen erfolgt über die Perimeterebene. Der Datenaustausch erfolgt immer über aktive Sicherheits-komponenten.
- Schutzzonenübergreifende Kommunikation von Anwendungen erfolgt immer über die Ebene 2, d.h. der Sicherheitsinfrastruktur (Perimeterschutz).
- Schutzzonen sind durch separate Hardware oder andere vergleichbare Isolierungsmechanismen abzubilden.
- Aufbau eines Hypervisorclusters pro Schutzzone oder Nachweis eines entsprechenden Isolierungsmechanismus.
- Physikalische oder vergleichbar getrennte LAN-Anbindungen der Schutzzonen.
- Für polizeiliche Verfahren sind eigene Schutzzonen zu bilden.
- Applikations-, Web- sowie fachliche Querschnittsdienste werden für jede Schutzzone getrennt bereitgestellt.
- Zugriffsrichtung ergibt sich aus dem Ranking der Schutzzonen (sicher nach unsicher).
- Unter Beachtung des Rankings der Schutzzonen kann auch eine gemeinsame Datenhaltung über Schutzzonen hinweg beantragt werden.
- Datenhaltungskomponenten sind grundsätzlich von Anwendungskomponenten mittels Paket-filter zu trennen.
- Unter Beachtung des Ranking der Schutzzonen erfolgt die Separierung der Infrastruktur für die Schutzzonen physikalisch, per Hypervisor oder durch andere Isolierungsmechanismen.

DMZ / DMZen untereinander

- Anwendungen werden in DMZ(en) betrieben.
- DMZen werden mittels Hypervisor-Firewall oder durch klassische Firewall-Infrastrukturen (siehe Vorgaben zur Perimeter-Ebene) abgebildet.
- Es können vLAN innerhalb der Schutzzone für die DMZ(en) genutzt werden.
- Für jeden Mandanten wird eine eigene DMZ für Applikations-, Web-, und fachliche Querschnittsdienste betrieben (siehe Abbildung 11).

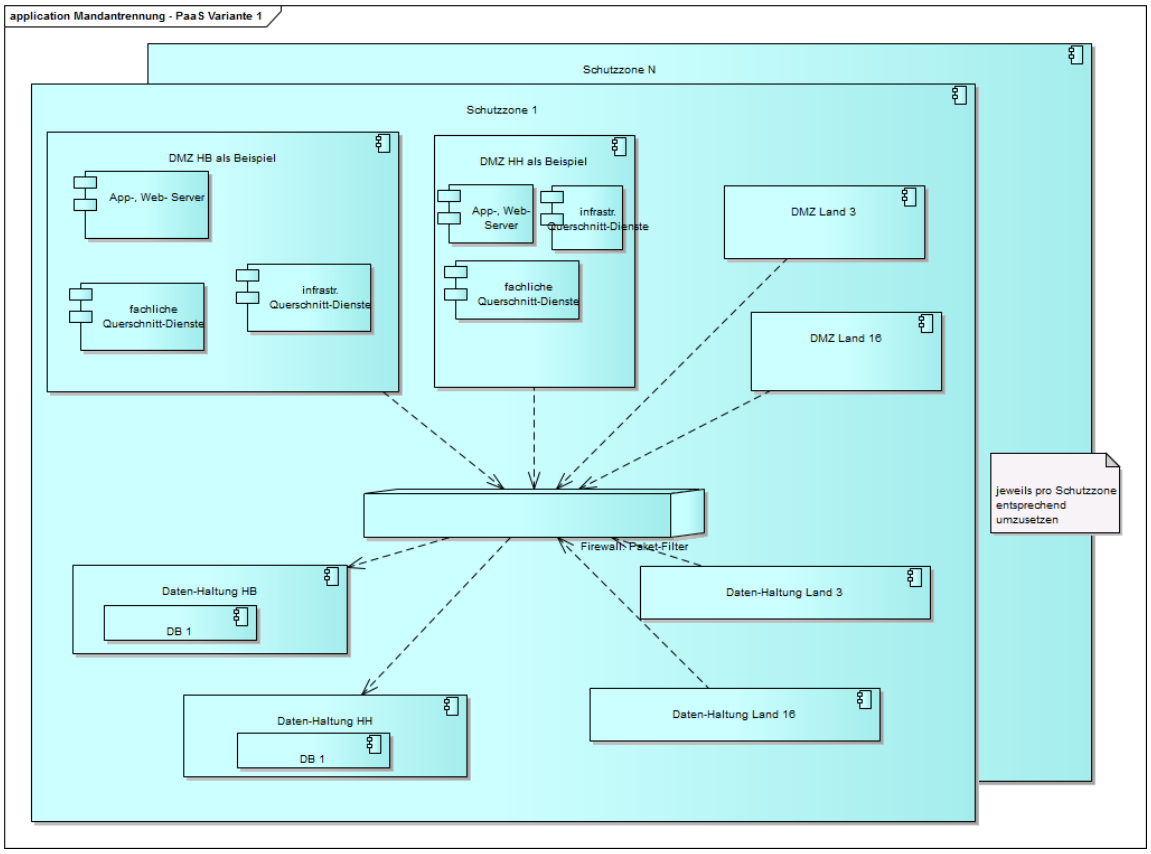

Abbildung 11: Mandantentrennung PaaS - Variante 1

Mandantenübergreifende Nutzung von DMZen für Applikations-, Web- und fachliche Querschnittsdienste unter der Voraussetzung, dass eine ausreichende Isolierung (fachlich, administrativ und infrastrukturell) der einzelnen Mandanten sichergestellt ist (siehe Abbildung 12).

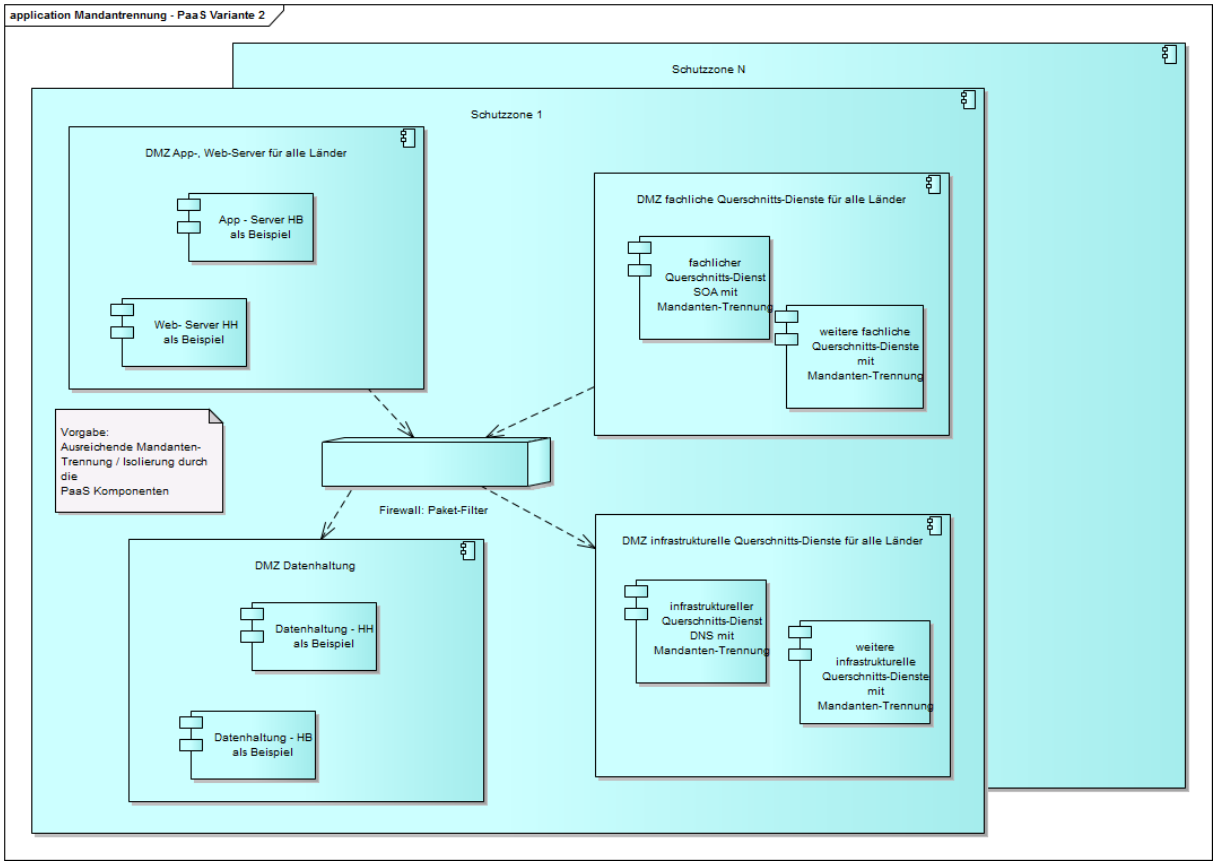

Abbildung 12: Mandantentrennung PaaS - Variante 2

- Anwendungen innerhalb einer Schutzzone kommunizieren, wenn sie in verschiedenen DMZen betrieben werden, über einen externen Paketfilter oder über die vom Hypervisor bereitgestellte Firewall. Die Kommunikation zwischen DMZen innerhalb einer Schutzzone verläuft nicht zwingend über weitere aktive Sicherheitskomponenten der Perimeterebene (Ebene 2).
- Für jeden Mandanten wird eine eigene DMZ für die Datenhaltung/Datenbanken betrieben bzw. bei gemeinsamer Datenhaltung muss eine vergleichbare Isolierung der Mandanten nachgewiesen werden.
- Ein Datenaustausch innerhalb der Datenhaltung/Datenbank DMZ ist nicht erlaubt sondern muss immer durch Anwendungen/Dienste erfolgen.
- Der Verwendung von „nativer Hardware“ für einen Grid-Ansatz wird zugestimmt, wenn eine dem Hypervisor vergleichbare Isolierung der Mandanten nachgewiesen wird.

Anlage 4: Ebene 4: IT-Infrastruktur

Gefährdungen

- Kompromittieren durch fehlenden Trennungsmechanismus.
- Fehlkonfiguration der Storagekomponenten, Computenodes, Netze, infrastrukturellen Querschnittsdienste beeinträchtigt alle Mandanten.
- Ausfall der Storagekomponenten, Computenodes, Netze, infrastrukturellen Querschnittsdienste (Hardware) beeinträchtigt alle Mandanten.
- Kopplung der Mandanten durch konzeptionelle Schwächen im Trennungsmechanismus.
- Fehler in der Komponente, die die logische Trennung durchführt.
- Kompromittieren durch eine Kopplung der Storagekomponenten, Computenodes, Netze, infrastrukturellen Querschnittsdienste von mehreren Mandanten durch eine zentrale Administration der Storagekomponenten, Computenodes, Netze, infrastrukturellen Querschnittsdienste.
- Kompromittieren durch eine Kopplung der Storagekomponenten, Computenodes, Netze, infrastrukturellen Querschnittsdiensten von mehreren Mandanten durch gemeinsame Nutzung (Konsolidierung) von fachlichen und infrastrukturellen Querschnittsdiensten.
- Diebstahl oder Änderung von Nutzdaten.

Maßnahmen

- Storagekomponenten, Computenodes, Netze, infrastrukturelle Querschnittsdienste sind pro Schutzzone durch separate Hardware oder andere vergleichbare Isolierungsmechanismen abzubilden: Anbei Beispiele für SAN, NAS und Netz:
    - SAN: LUN-Binding, LUN-Masking, Soft-Zoning
    - NAS/iSCSI: über Hypervisor ohne Separierung, sonst Separierung über vLAN
    - User-Netz: Separierung über vLAN
    - SDN mit White-Listing
    - vSAN mittels Namespace
    - Nodes mittels Isolierter Segmente, Host-Gruppen.
- Die Anbindung der Hypervisor-Cluster an den genutzten Storage erfolgt über Paketfilter bzw. durch SDN Isolierung.
- Anbindung der Ebene 3 an die Ebene 4 erfolgt entkoppelt vom User-Netz über eigene LAN/vLAN-/SDN-Strukturen mit entsprechenden Isolierungsmechanismen.

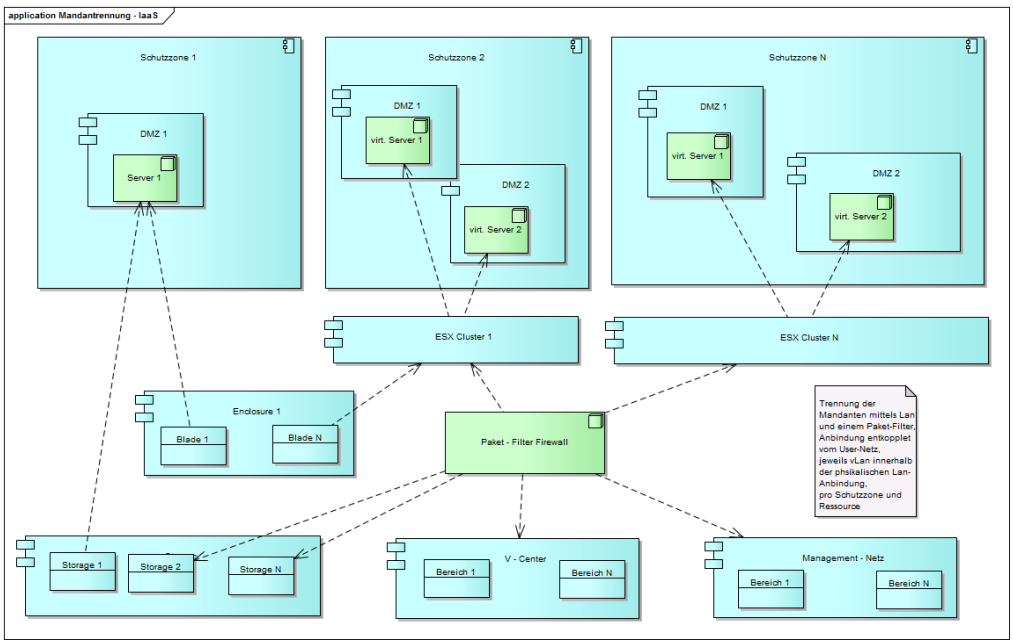

Abbildung 13: Mandantentrennung IaaS

Anlage 5: Erweiterte Anforderungen an die Administration der Ebenen 1-4

Alle Ebenen

- Der Zugriff auf die Infrastruktur muss in einem Rechte-und-Rollen-Attribute-Konzept geregelt sein und muss eine Zwei-Faktor-Authentisierung vorsehen.
- Die Wirksamkeit der Maßnahmen, um die Sicherheitsinfrastruktur vor unbefugten Zugriffen abzusichern, sollte zyklisch durch einen Penetrationstest überprüft werden. Gefundene Schwachstellen sollten zeitnah behoben werden.
- Eine mandantenübergreifende Administration durch den Dienstleister ist grundsätzlich möglich. Natürlich hat hierbei der Zugriff über personifizierte Accounts zu erfolgen. Es ist eine Trennung root und anderen privilegierten Accounts sowie eine sichere Protokollierung der Zugriffe (Nachvollziehbarkeit) sicherzustellen.
- Der Verbindungsaufbau erfolgt nur von den Admin-Clients in die Schutzzone(n), nicht umgekehrt.
- Der Administrator-Zugriff erfolgt per Paketfilter-Trennung beispielsweise Terminal-Server-Anbindung (Terminal Server-Farm mit mandantenbezogener Zuordnung der Terminal Server).

Nur Ebene 1

- - - O H N E - -

Nur Ebene 2

- Die Administration der Ebene 2 erfolgt ausschließlich durch den Dienstleister.

Nur Ebene 3

- In jeder Schutzzone steht ein eigener Infrastrukturserver mit zentralen Administrations- und Konfigurationswerkzeugen für die Verwaltung. Dieser Server hat Zugriff auf die in der Schutzzone aufgespannten DMZen und den in diesen installierten Datenbankservern (Datenhaltung), Web-, Applikationsservern sowie fachlichen Querschnittsdiensten.
- Die Nutzung/Verwaltung von Services über DMZen durch ein Tool wird zugestimmt, wenn diese durch den Dienstleiter begründet beantragt werden. Hierfür ist der Nachweis einer vergleichbaren Isolierung (fachlich, administrativ und infrastrukturell) der Mandanten/Service zu erbringen.
- Erfolgt die Administration ausschließlich durch den Dienstleister und erfolgt eine sichere Protokollierung der Administrationszugriffe mit personenbezogener Zuordnung, kann auf den Einsatz eines PAM (privilegiertes Account Management) verzichtet werden.
- Bei einer Mischform der Administration durch Dienstleister und Kunde, z.B. in der Ebene 3, ist der Zugriff auf die Komponenten mittels PAM zu steuern.
- Der Kunden-Administrations-Zugriff erfolgt mittels Token (föderative Identitäten-Management (IDM)) über User-Daten-Netz mit Zwei-Faktor-Authentifizierung und Prüfung der Identität und Rechte.

Nur Ebene 4

- Die Administration der Ebene 4 erfolgt ausschließlich durch den Dienstleister.
- Der Administrator-Zugriff auf infrastrukturelle Querschnittsdienste im Bereich IaaS und PaaS erfolgt generell per Paket-Filter-Trennung und Terminal-Server-Anbindung (Terminal Server-Farm mit mandantenbezogener Zuordnung der Terminal Server). Die Verbindungs-Richtung erfolgt immer nur vom Admin-Client in die Schutzzone.
- Der Administrator-Zugriff auf infrastrukturelle Querschnittsdienste im Bereich IaaS und PaaS durch den Dienstleister (IaaS) und den Kunden (PaaS) benötigen eine Steuerung mittels Cloud-SW zur Verfügung gestellter Zugriffswege inkl. Protokollierung sowie Isolierung.

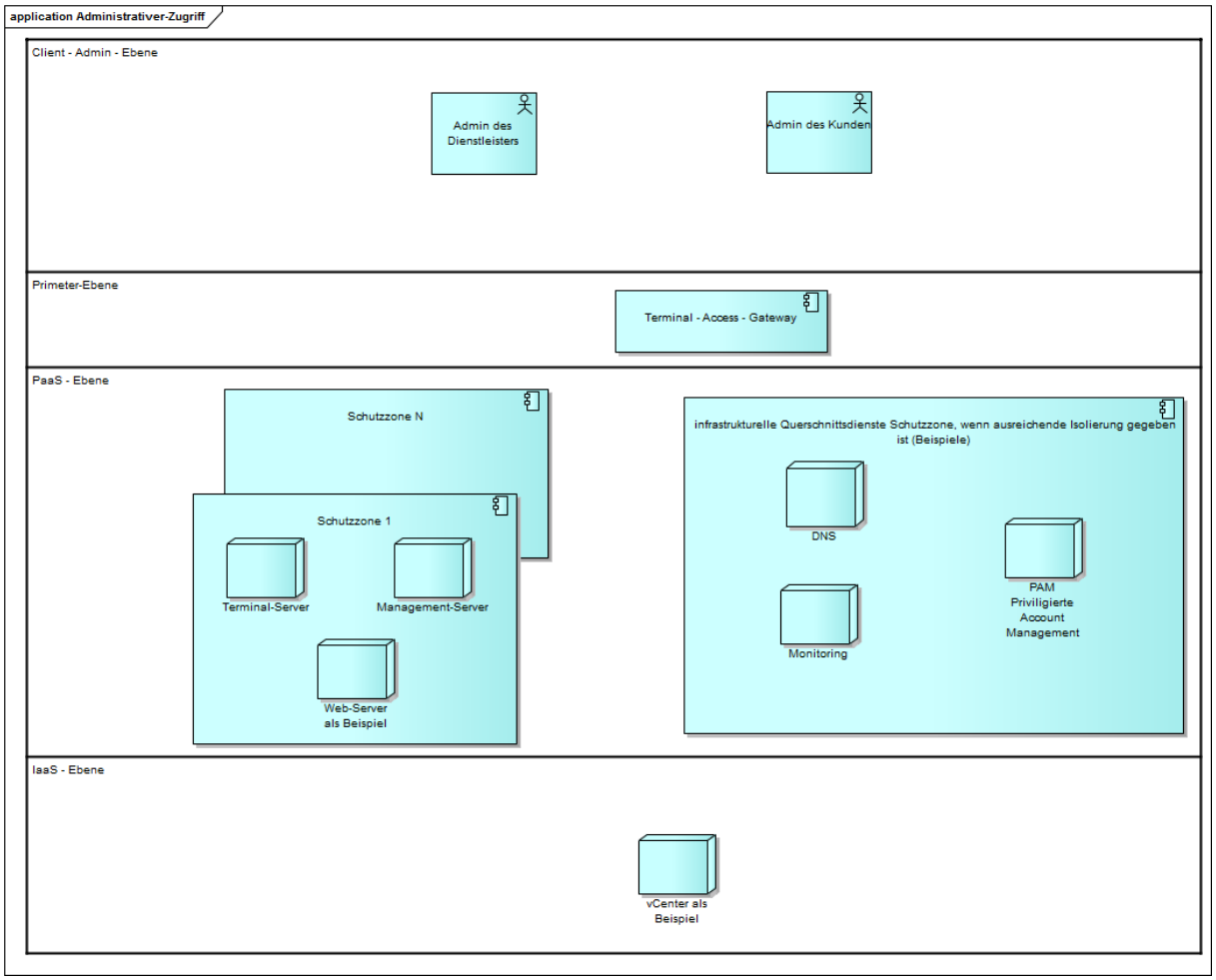

Abbildung 14: Komponenten für einen administrativen Zugriff über die Ebenen hinweg

Anlage 6: Beispiele einer Isolierung

a) Monitoring:

Das Beispiel beschreibt das technische Monitoring von Infrastrukturkomponenten über Ebenen und Schutzzonen hinweg auf eine zentrale Monitoring Komponente.

Hierbei befinden sich z.B. in den DMZen entsprechende Monitoring-Agents. Die Monitoring Agents (pro Server in den DMZen) senden an den Monitoring Reverse Proxy, welcher sich in Ebene 3 befindet. Der zentrale Monitoring-Server, welcher sich z.B. in Ebene 4 befindet, holt die Daten von den jeweiligen Monitoring Reverse Proxy ab. Abhängig von der Bewertung des Ranking der Schutzzone kann ein Reverse Proxy für das Monitoring schutzzonenübergreifend genutzt werden. In diesem Beispiel kam die Bewertung zu dem Ergebnis, dass Schutzzone gelb und grün einen gemeinsamen ReverseProxy nutzen können, während zwingend für Schutzzone rot ein eigener ReverseProxy zu nutzen ist.

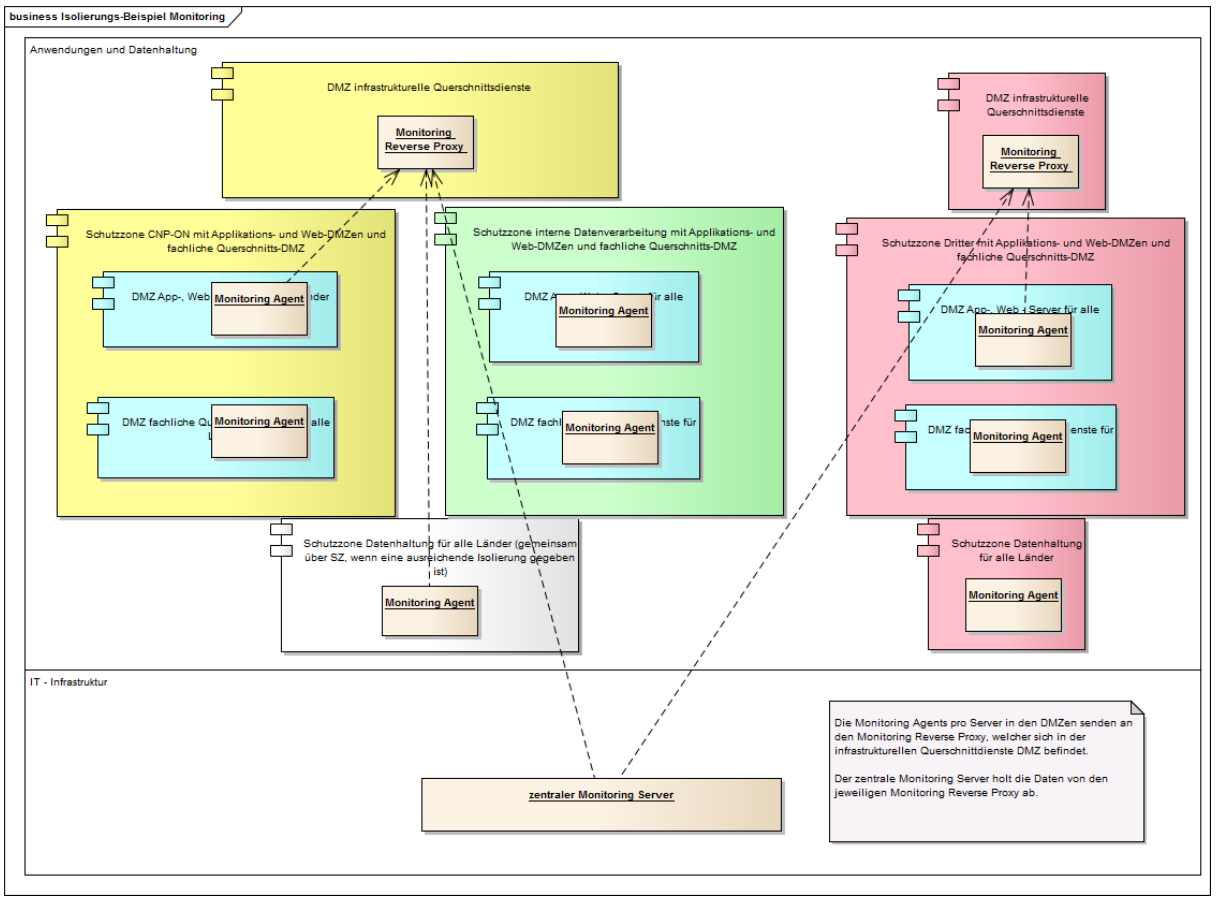

Abbildung 15: Beispiel Monitoring

b) Datenaustausch:

Das Beispiel beschreibt den fachlichen Bedarf eines Filedatentransfers zwischen verschiedenen Schutzzonen. Hierbei handelt es sich um Schutzzonen unterschiedlichen Rankings. Fachlich besteht die Anforderung, Daten aus einer weniger vertrauenswürdigen Schutzzone in eine höherwertige Schutzzone zu transferieren. Entsprechend des erfolgten Ranking verhindern aktive Sicherheitskomponenten zwischen den Schutzzonen aber diese Kommunikation. Zur Lösung dieser Problemstellung wird der u.a. Mechanismus genutzt.

Hierbei befinden sich z.B. in den DMZen entsprechende Transfer- und Jobsteuerungs-Agents. Diese Agents sorgen in Verbindung mit der zentralen Transfer- und Jobsteuerungskomponente

dafür, dass die tatsächliche Kommunikationsrichtung entsprechend den zuvor gemachten Vorgaben entspricht, d.h. die Daten werden von der höherwertigen Schutzzone aus abgeholt.

Die Agents erhalten von dem zentralen File-Transfer- und Job-Steuerungs-Server ihren Auftrag entsprechend des zu transferierenden Objektes und der definierten Job-Kette. Der zentrale File-Transfer- und Job-Steuerungs-Server steuert die Aufträge und die Kommunikationsrichtung.

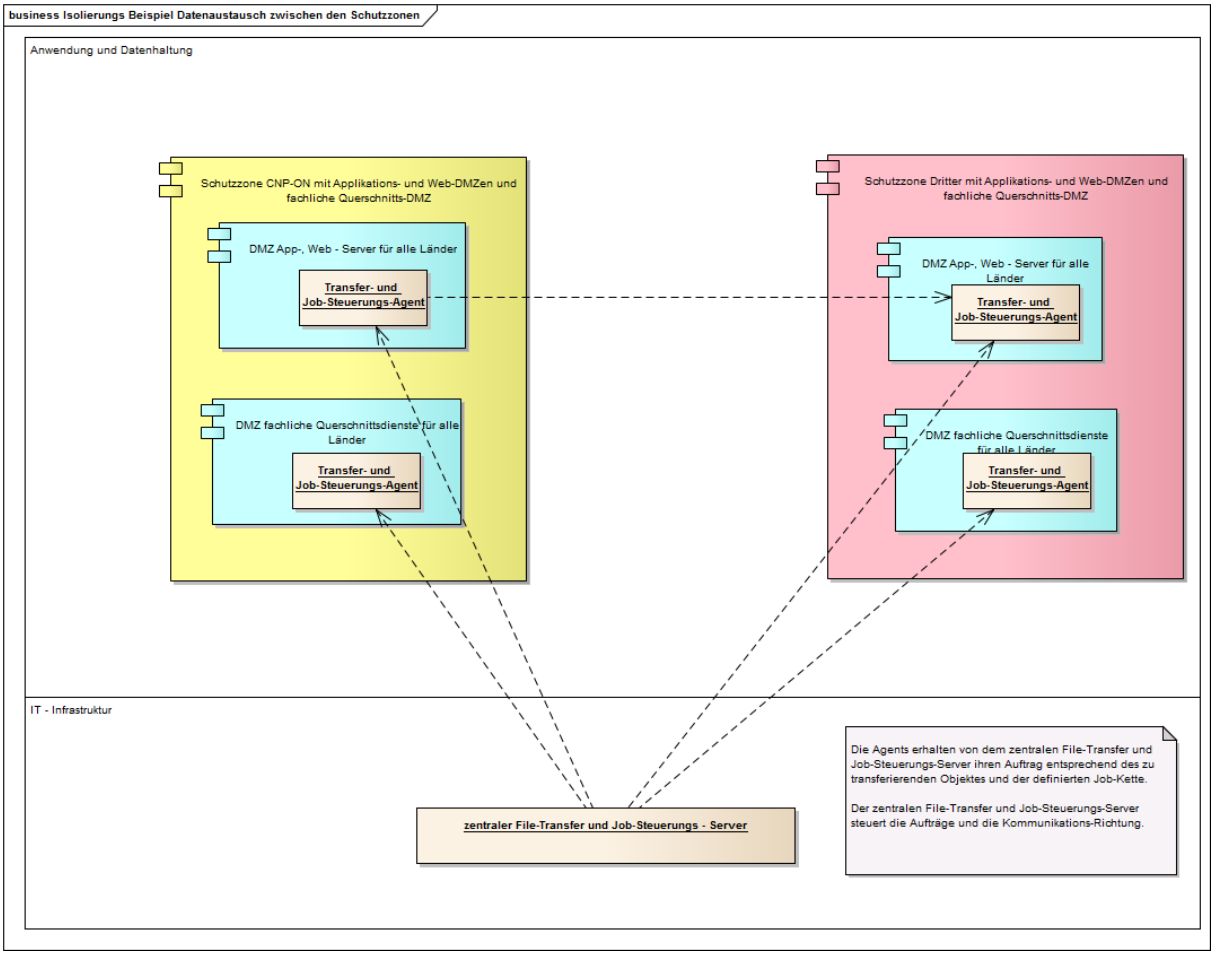

Abbildung 16: Beispiel Datenaustausch

Anlage 7: Erläuterungen zur Referenzarchitektur an Hand von Beispielen

Prinzipieller Aufbau

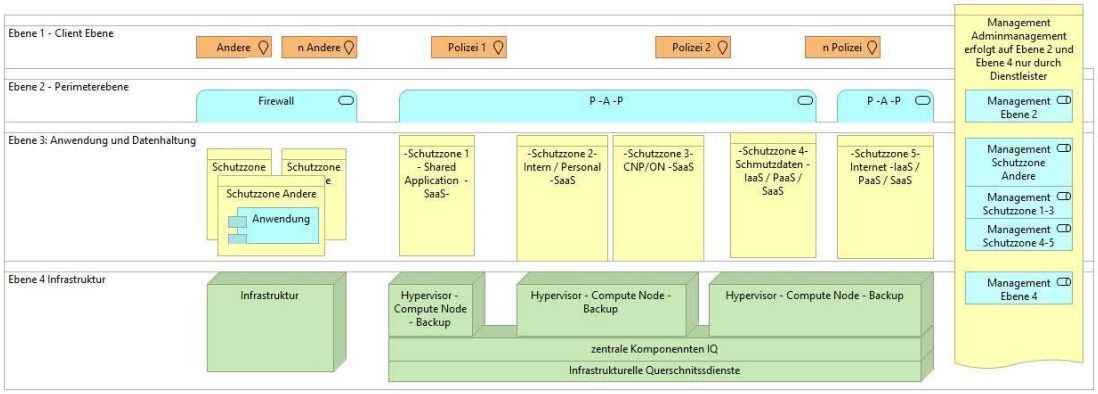

Abbildung 17: Darstellung prinzipieller Aufbau von Schutzzonen für polizeiliche Verfahren

Ebene 2: Die in der Perimeterebene genutzten Komponenten für die Schutzzone Internet sowie SharedApplikation (ShA) Dritter ist hardwaregetrennt von der in der Perimeterebene genutzten Komponenten für die anderen Schutzzonen der Polizei. D.h. für die Polizei wird dediziert HW für die Schutzzone Internet sowie Schutzzone ShA/intern/CNP-ON und Schmutzdaten bereitgestellt. Die Nutzung der gemeinsamen Komponente in der Ebene 2 erfolgt bei Sicherstellung einer ausreichenden Isolierung.

Ebene 3:

Schutzzone-Dritter

Links wird die Infrastruktur Dritter (Nicht-Polizeien) über die Ebenen 1-4 dargestellt. Es handelt sich hierbei nicht um polizeiliche Infrastruktur oder Verarbeitung polizeilicher Informationen, d.h. es wird hier eine von der Polizei getrennte Infrastruktur bereitgestellt. Diese Trennung zieht sich auch durch Management, Administration sowie fachliche und infrastrukturelle Querschnitts-dienste. Nichts desto trotz könnten Mitarbeiter der Polizei auf Anwendungen wie Reisekosten, Reiseplanung etc. zugreifen. Storage Ressource wie SAN oder NAS können bei einer ausreichenden Isolierung, z.B. per getrennter Anbindung, gemeinsam genutzt werden. Entsprechendes gilt auch für Backup-Infrastruktur.

In der Mitte werden die polizeilichen Infrastrukturen dargestellt, d.h. Betreiber ist hier die Polizei und es werden polizeiliche Daten verarbeitet. Hier wird unterschieden zwischen 5 Schutzzonen:

1. SharedApplikation mit Zugriff Dritter: Hier werden als SaaS Anwendungen/Services betrieben, auf die auch Dritte zugreifen. Die Anwendung liegt in der Hoheit der Polizei, aber es können auch Nicht-Polizeien zugreifen.
2. Schutzzone intern werden als SaaS polizeinterne Informationssysteme gehostet, die keine Kommunikation nach Extern haben.
3. Schutzzone CNP-ON werden als SaaS polizeiliche Informationssysteme betrieben, die eine Kommunikation nach Extern haben.
1. In der Schutzzone Schmutzdaten werden als SaaS, PaaS oder IaaS Anwendungen betrieben, die potentiell Schmutzdaten enthalten, d.h. deren Daten Schadcodebehaftet sein können oder aus unsicheren Quellen stammen.
2. In der Schutzzone Internet werden als SaaS, PaaS oder IaaS Anwendungen betrieben, die eine Anbindung ans Internet haben.

Die Kommunikation innerhalb einer Schutzzone erfolgt über einen Paketfilter. Dies kann aus der Ebene 2 stammen. Es ist aber auch möglich, durch ein Virtualisierungsprodukt oder anderen Isolierungsmechanismen, diesen auch innerhalb der Ebene 3 bereitzustellen. Die Kommunikation

zwischen Schutzzonen erfolgt zwingend über die Perimeterebene mit der im Dokument beschriebenen Richtung des Verbindungsaufbaus.

Ebene 4: In der Ebene 4 ist für die Schutzzone ShA ein von den restlichen Schutzzonen getrennter Hypervisor vorzusehen. Bei Vorhandensein einer ausreichenden Isolierung ist eine gemeinsame Nutzung eines Hypervisor für die Schutzzone intern und CNP-ON möglich, ebenso für die Schutzzone Schmutzdaten und Internet.
Das Management der Ebene 2 und 4 erfolgt ausschließlich durch den Dienstleister. Bei PaaS und IaaS erfolgt der Zugriff auf die Infrastruktur auch für die Administration über das Kundennetz (ggf. ein separates Kundennetz), nicht über das Management-LAN des Dienstleisters.

SharedApplikation im Bereich der polizeilichen Infrastruktur

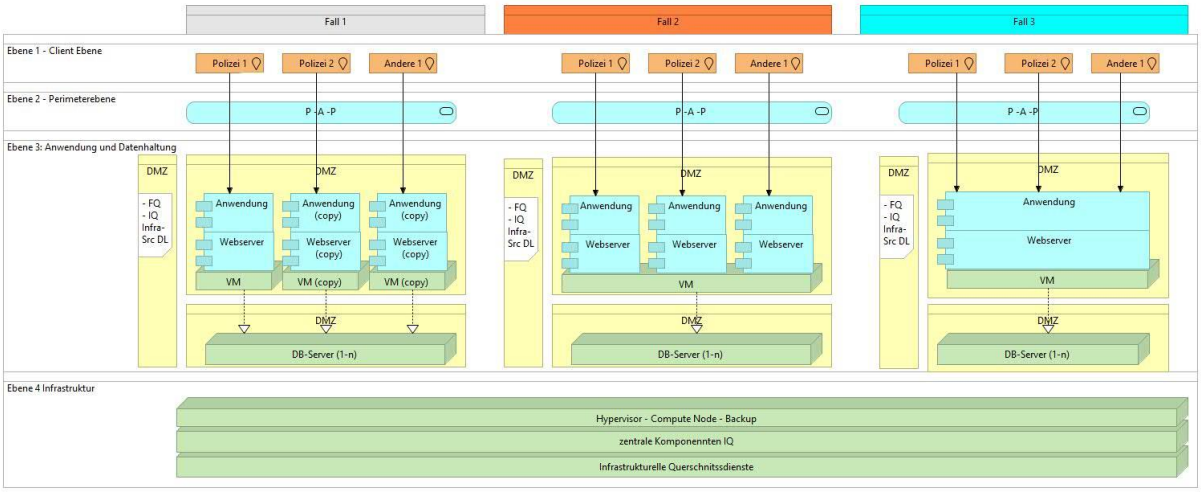

Abbildung 18: Darstellung prinzipieller Aufbau Shared Application

Fall 1: Mit der Möglichkeit einer Konsolidierung aber der größtmöglichen Trennung zwischen verschiedenen Mandanten werden hier eigene VM, eigene WebServer und eigene Anwendungen/ Anwendungskomponenten pro Mandant bereitgestellt. Getrennte oder gemeinsame Datenhaltung ist möglich, wenn dies durch die Anwendung unterstützt wird.

Fall 2: In diesem Beispiel kann eine gemeinsame VM genutzt werden. Es werden hier pro Mandant ein eigener WebServer und eigene Anwendungen/Anwendungskomponenten bereitgestellt. Getrennte Datenhaltung oder gemeinsame DB sind möglich, wenn dies durch die Anwendung/ Anwendungskomponenten unterstützt wird.

Fall 3: In diesem Beispiel geht die Konsolidierung noch einen Schritt weiter. Hier erfolgt die Mandantentrennung innerhalb der Anwendung – die Anwendung muss dies unterstützen, z.B. über gut implementierte Rechte- und Rollenkonzepte. Getrennte Datenhaltung oder gemeinsame DB sind auch hier möglich, wenn dies durch die Anwendung unterstützt wird.

=> Es muss mindestens Fall 3 umgesetzt sein unter den genannten Voraussetzungen einer ausreichenden Isolierung.

Schutzzone intern sowie CNP-ON am Beispiel einer FAT-Client Anwendung

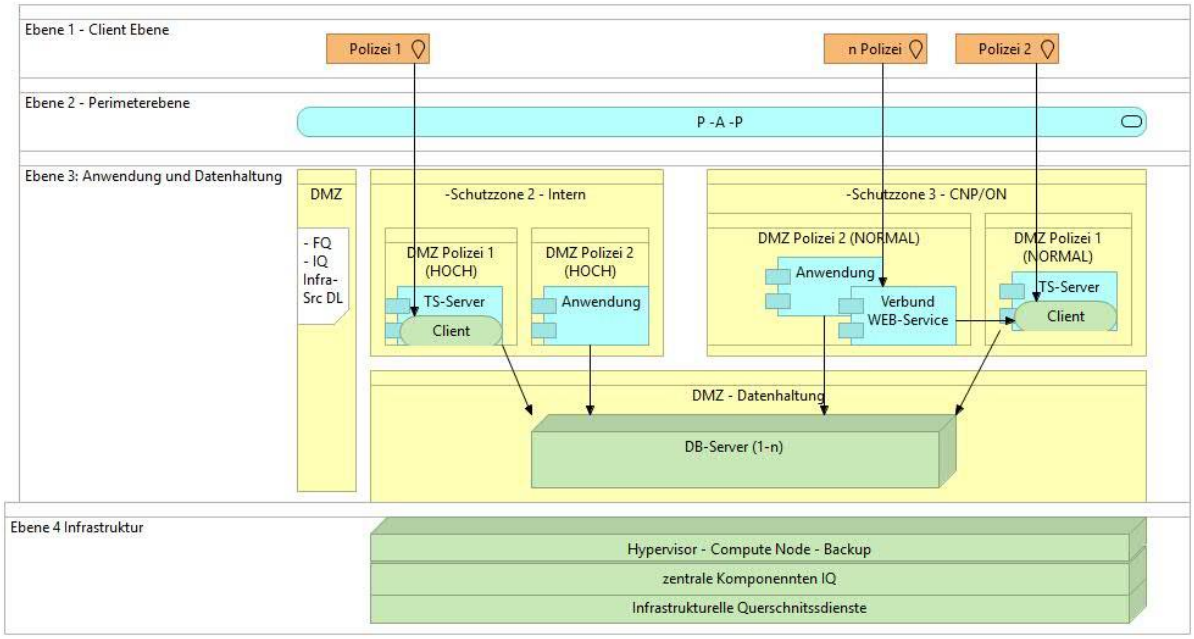

Abbildung 19: Darstellung prinzipieller Aufbau FAT-Client-Anwendung

Ebene 2:

In der Ebene 2 können Komponenten gemeinsam genutzt werden, wenn diese eine ausreichende Isolierung pro Mandant gewährleistet.

Ebene 3:

Die Schutzzone intern sowie Schutzzone CNP-ON können sich einen Hypervisor teilen. Ebenso ist es hier möglich, fachliche und infrastrukturelle Querschnittsdienste, Terminalserver oder die Datenhaltung gemeinsam zu nutzen. So wird gerade für den Zugriff von FAT-Client-Anwendungen die Nutzung von Terminalservern empfohlen, um hier einen 3-Tier-Architektur-Ansatz zu erreichen. Auch die Terminalserverumgebung kann gemeinsam genutzt werden, hier wird auf eine sinnvolle Trennung innerhalb der TS-Umgebung verwiesen.

Eine DMZ gemeinsame Datenhaltung über beide Schutzzonen hinweg ist möglich, soweit eine ausreichende Trennung der Daten durch die Umgebung gewährleistet ist.

In dem oben dargestellten Beispiel greift ein FAT-Client direkt auf die Datenbank zu. Eine sicherere Lösung wäre hier die Positionierung eines Connectionmanagers (Proxy-Funktion) in der DMZ der Polizei 1 bzw. der Polizei 2, um einen Zugriff direkt auf die DB zu vermeiden. Der Zugriff kann auch über Terminalserver realisiert werden, so dass der FAT-Client dort innerhalb einer DMZ in der Ebene 3 steht.

Über ein Verbundwebservice ist eine Kommunikation zur Zentralstelle möglich. Hier kann auch ein XML-Gateway in Ebene 2 die Kommunikation absichern. Es ist auch hier ein personifizierter Zugriff mittels Accessmanager zur Erhöhung der Sicherheit angeraten (Authentifizierung).

Schutzzone Schmutz sowie Internet

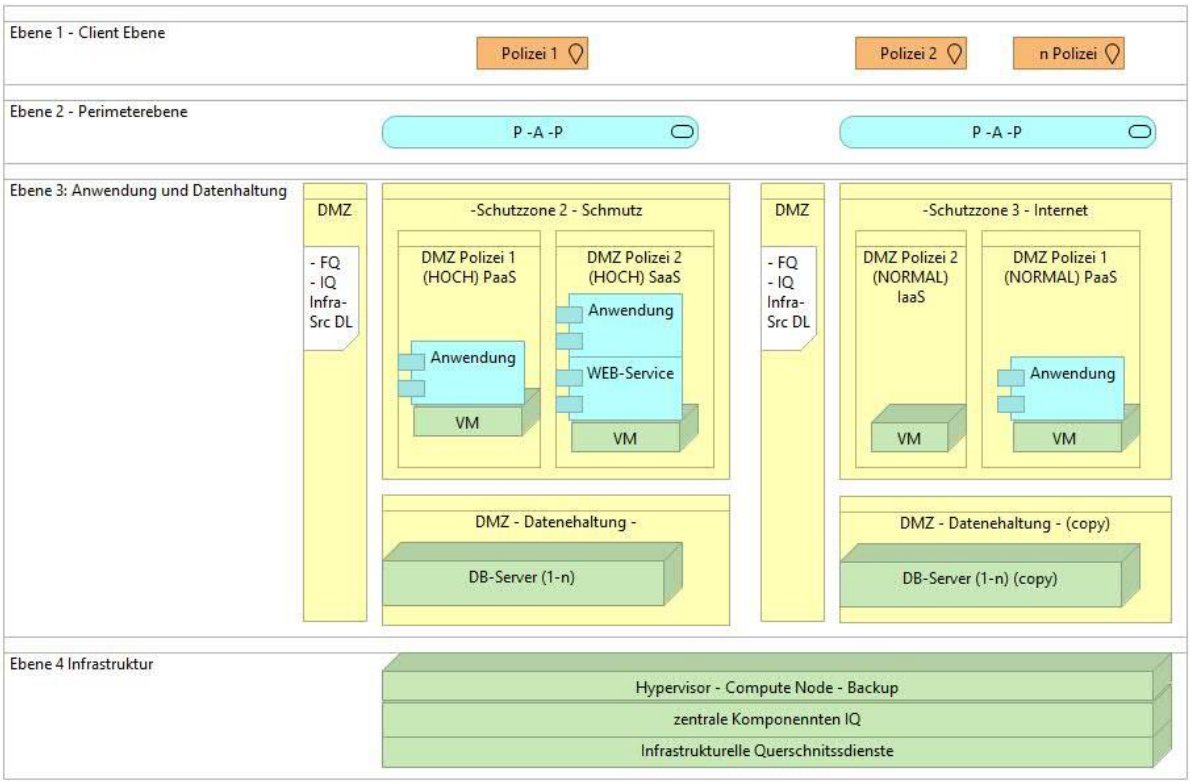

Abbildung 20: Darstellung prinzipieller Aufbau Schutzzonen Schmutzdaten und Internet

- Eine ausreichende Isolierung vorausgesetzt wird hier die Möglichkeit gesehen, für beide Schutzzonen eine gemeinsame Hypervisor-Infrastruktur zu nutzen. Eine weitere Konsolidierungsmöglichkeit wird hier nicht gesehen. Dies bedeutet, dass alle anderen Komponenten der Ebene 2, 3 und 4 über getrennte Hardware bereitgestellt werden muss. Auch die fachlichen und infrastrukturellen Querschnittsdienste sind hier getrennt bereitzustellen und können nicht gemeinsam genutzt werden. Es werden hier keine ausreichenden Isolierungsmechanismen gesehen, die eine Gefährdung aus dem Internet vergleichbar einer physikalischen Bereitstellung entsprechen würde.
- Im Falle von SaaS erfolgt die Administration rein durch den Dienstleister.
- Im Falle von PaaS stellt der Dienstleister VM, Betriebssystem und Datenbank, Web-Server bereit, der Kunde administriert die Anwendung.
- Im Falle von IaaS stellt der Dienstleister VM bereit, der Kunde ist für Betriebssystem, Webserver sowie Anwendung zuständig.

Kapitel 3: Software-Defined-DataCenter SDDC

Durch die Konsolidierung von IT-Komponenten können zuvor durch „Hardware“ getrennte IT-Verbünde, auch verschiedener Mandanten, zusammengeführt werden. Dieser Umstand erfordert deshalb eine angepasste Bewertung von Cloud-Technologien sowohl aus Gründen der Informationssicherheit als auch des Datenschutzes.

Neben angestrebten finanziellen und personellen Einsparungen bieten Cloud-Technologien auch Vorteile hinsichtlich der Skalierung von IT-Systemen. So lassen sich beispielsweise über das prognostizierte Maß hinausgehende Ressourcenbedarfe sehr dynamisch, mit einem hohen Automatisierungsgrad anpassen oder Hardwareausfälle unproblematisch begegnen.

Fachliche Anforderungen können durch den Kunden schnell und flexibel realisiert werden, ohne Genehmigungsprozesse oder Vorlauf beim Dienstleister berücksichtigen zu müssen, da Prozesse, Richtlinien und Templates bereits genehmigt sind.

Konkret bieten Cloud-Technologien in Verbindung mit einer hohen Automatisierung und Standardisierung neuen Möglichkeiten, sehr selektive IT-Sicherheit für Services umzusetzen.

In diesem Dokument werden SDDC-Infrastrukturen für Cloud-Umgebungen betrachtet.

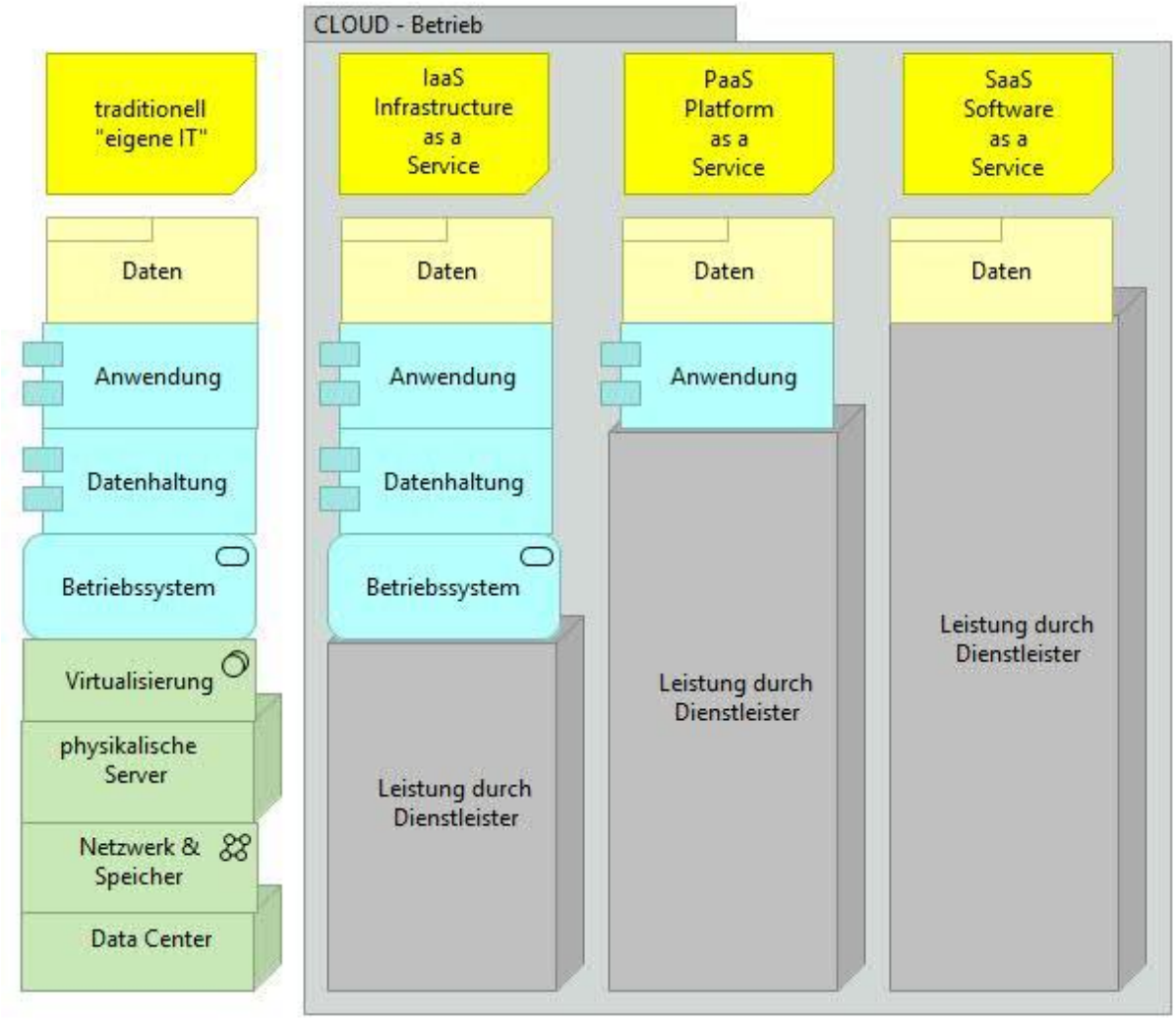

Abbildung 21 Darstellung Entwicklung traditionelle IT hin zu Cloud

Nicht Gegenstand der Betrachtung sind derzeit noch Plattformsteuerungstools für Cloud-Umgebungen.

IT-Sicherheitsbetrachtungen für den Bereich Plattformsteuerungstools zur Verwaltung der Services werden in einer Fortschreibung des Dokuments beschrieben. Ebenso der erforderliche Umbau fachlicher Applikationen Richtung Mikroservice und die damit verbundenen neuen Ansätze im Bereich continous integration (ci) und continuous deployment (cd). Neue Ansätze zur Zusammenarbeit innerhalb der Abteilung IT (devops) müssen ebenso noch betrachtet werden.

3.1 Erweiterte Begrifflichkeiten

In Ergänzung zu den im übergeordneten Dokument definierten Begrifflichkeiten werden hier die Änderungen aufgezeigt, die sich durch SDDC ergeben.

Ebenen
Durch Nutzung von software-definierten Technologien verlagern sich Funktionalitäten.

Diese, vormals in Ebene 2 wahrgenommen, können bei Nutzung von software-definierten Funktionalitäten auch in die Ebene 3 oder 4 verlagert werden. Hierbei ist zu beachten, dass die Funktionen in der Ebene 4 wirken und somit transparent für die Ebene 3 sind oder aktiv in der Ebene 3 wirken (Verschlüsselung oder Protokoll-Mapping SOAP/Rest).

Allgemein können Sicherheits-Funktionen/Komponenten in allen Ebenen zum Teil die gleiche Funktion erzielen:

- In der Ebene 2 kann mittels aktiven Sicherheitskomponenten Netzsegmentierung erfolgen und Service mittels API-Management gekapselt bzw. geprüft werden.
- Software-Defined-Network (SDN) kann mittels Edge-, verteilten FW-Komponenten und integrierten 3 Party Komponenten oder API-Management entsprechende Funktionen zur Verfügung stellen.
- In der Ebene 3 können durch Komponenten-FW (Datenbank-FW oder Datenhaltungs-Security-Layer) im Bereich der Datenhaltung weitere Sicherheit/Isolierung erzeugt werden.

Service-Schutz-Gruppen
Bei Einsatz von software-definierten Lösungen gewinnt die Service-Isolierung einen noch stärkeren Stellenwert. Sicherheit wird auf logischer Basis mittels Service-Schutz-Gruppen und ihnen zugeordneten Policies (Regelwerk) erzielt.

Diese Service-Schutz-Gruppen bilden auch Funktionalitäten aus der Ebene 2 ab, in dem sie Mechanismen der Isolierung (Paket-Filter, Protokoll-Type-Prüfung, API-Security etc.) nutzen. Die Service-Schutz-Gruppen werden über SDDC Mechanismen z.B. mittels SDN ausgebildet.

Hierbei sind folgende Definitionen jeweils für IaaS und PaaS notwendig:

- Security Policies definieren WIE der Schutz aussehen soll.
- Security Policy Gruppen definieren WAS geschützt werden soll.

SDN
Software-Defined Networking verbindet die physikalische Netzebene mit der logischen Netzebene über SDN Edge-Komponenten. Datenflüsse werden innerhalb des SDDC über logische/software definierte Netze gesteuert.

Die SDN-Komponenten ermöglichen hierbei eine kleinteilige Netzsegmentierung. Dies ermöglicht die Umsetzung der Service-Schutz-Gruppen.

Die SDN Funktion des Hypervisors bietet regelbasierte Sicherheit für die Services. Sie stellen eine verteilte Firewall dar. Es werden u.a. Policies erstellt, verwaltet und überwacht.

Es existieren hier u.a. SDN-Management-, SDN-Control- sowie SDN-Data-Komponenten entsprechend dem Overlay-Standard.

SDN-Edge
SDN Edge stellen den Übergang zwischen dem physikalischen Netz und dem software-definierten Netz dar.

Software-Defined Compute und –Storage (SDC und SDS)

Hier erbringen die jeweiligen Subsysteme in Verbindung mit dem Hypervisor (Cluster) die Sicherheits-Mechanismen.

SDDC

Das Software-Defined-Data-Center stellt zentrale Automatisierungs-, Orchestrierungs-, Monitoring- und Logging-Service für die Cloud-Umgebung zur Verfügung. Es bietet Sicherheitsmechanismen mittels IaaS , PaaS und Querschnittsdienst-Funktionen.

Hierbei können Sicherheits-Policies und Gruppen in den Ebenen 2-4 definiert werden.

Firewall

Es wird unterschieden zwischen

- Physikalischer Firewall
- Edge Firewall (siehe SDN-Edge)
- Verteilter Firewall (siehe SDN).

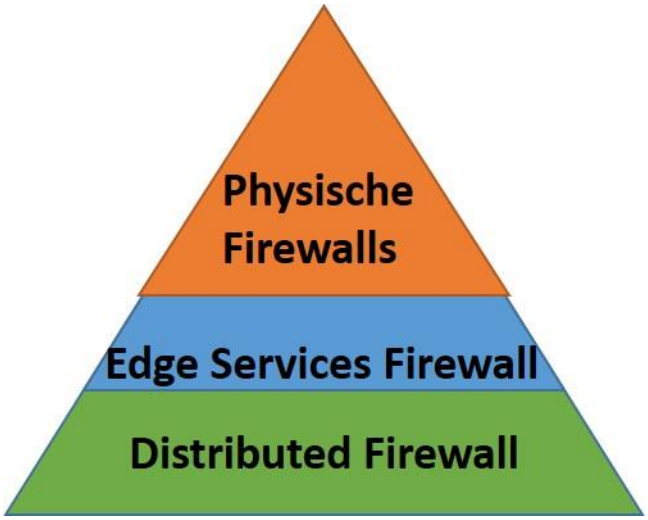

Abbildung 22: Firewall-Pyramide

Policies sind:

- Netzwerk basiert (Nutzung von z.B. IP Adressen durch Border-FW oder SDN-Edge)
- Infrastruktur basiert (Nutzung von logischen Sicherheitsgruppen wie z.B. ein Cluster mittels verteilter Firewall)
- Service basiert (Nutzung von Service Gruppen z.B. Nachrichten-Struktur mittels API-Management).

3.2 Erweiterte Kernaussagen im Zusammenhang mit SDDC

Management

Alle über SDDC bereitgestellten Ressourcen (z.B. Storage) sowie Services werden über ein Management verwaltet. Die Managementinfrastruktur ist eine eigene Umgebung in einem separierten Netzsegment. Ebene 4 verwendet eigene Querschnittsdienste.

Sowohl Querschnittsdienste als auch Managementumgebung sind durch Firewallkomponenten zu trennen.

Der Admin-Zugriff auf die Management-Komponenten erfolgt mittels PAM (Privileged Account-Management) und mittels Terminalserver über aktive Sicherheitskomponenten. Der administrative Zugriff auf die Management-Komponenten ist zu überwachen sowie zu protokollieren.

Es wird ein selektives Rollenkonzept im Management (z.B. Rollen für Service-, Infrastruktur-Betrieb und Portfolio) umgesetzt.

Wenn eine SDDC /SDN Lösung mit einem zentralen Management für alle Komponenten der Ebene 2-4 angedacht ist, muss die Management-Umgebung durch Sicherheitskomponenten geschützt werden, sowohl Richtung Admin-Zugriff als auch Richtung der Service-Infrastruktur.

Des Weiteren gilt:

- Aus der Ebene 4 bereitgestellte Ressourcen sind zwischen Polizeien und Dritten logisch und sicher zu separieren. Dies erfolgt über die den Service-Schutz-Gruppen zugewiesenen Policies. Die anzuwendenden Policies richten sich nach der Schutzbedürftigkeit der Applikation bzw. Services. Hier sind Abstufungen hinsichtlich der gemeinsamen Nutzung von Ressourcen möglich.
- Eine gemeinsame Nutzung SDDC mit Dritten ist möglich. Die Trennung kann über SDN, Hypervisor-Trennung erfolgen. Eine ausreichende Isolierung zwischen den Services der Mandanten muss gegeben sein. Hierbei ist die Isolierung der Service-Schutz Gruppen maßgeblich.
- Durch SDN Edge Netzsegmentierung oder SDN-Regeln mittels verteilter Firewall können Sicherheitsfunktionen, die bisher aus Ebene 2 der Ebene 3 zur Verfügung gestellt wurden, jetzt durch Ebene 4 der Ebene 3 bereitgestellt (u.a. IDS/IPS, Schadcodeprüfung, Verschlüsselung) werden. Die Border-Firewall als Ebene 2 ist davon unberührt.
- Der Grad der Service-Isolierung wird durch die Sicherheits-Polices der Service-Schutz-Gruppen definiert.
- Die Ebene 2 übt die Funktion einer Border-Firewall aus, wenn externe Kommunikation, Kommunikation zu Partnern und Services – außerhalb des SDDC – stattfindet („Nord-Süd-Kommunikation“).
- In der Ebene 2 werden für die Nutzung der Sicherheitskomponenten Policies bereitgestellt. Die Nutzung der Policies für eine Kommunikation eines Service nach außen, wird über die zentrale SDDC-Umgebung zugeteilt. So werden für die Kommunikation eines internen Service mit einem externen Service vordefinierte Firewallregeln genutzt.

SDDC/SDN

Mandantenübergreifende Nutzung von DMZen / SDDC-Service-Trennung für Applikations-, Web- und fachliche Querschnittsdienste ist unter der Voraussetzung möglich, dass eine ausreichende Isolierung (fachlich, administrativ und infrastrukturell) der einzelnen Mandanten sichergestellt ist.

Bei einer SDDC / SDN Lösung ist jeder Service und jede Kommunikation zwischen den Services zu definieren und per SDN-FW zu prüfen. Der Grad der Prüfung hängt davon an, ob eine Schutzzone verlassen wird oder Services mehrere Mandanten mit einander kommunizieren. Entsprechend

werden weitere Sicherheitskomponenten in die Kommunikationskette zwischen den Services eingefügt (z.B. virtueller Paketfilter oder ALG oder Autorisierungsprüfung mittels Access-Management bzw. API-Management).

Monitoring

Bei einer SDDC Lösung mit zentralem Management inklusive einer zentralen Monitoring / Logging Funktionalität muss eine entsprechende Isolierung über alle zu überwachenden Komponeten gewährleistet sein. Hierbei sind die Ebenen-Übergänge möglichst zu vermeiden, d.h. jede Ebene führt ein explizites Monitoring & Logging durch.

3.3 Vorgehensweise Software Defined Datacenter - SDDC

- Festlegung der Service-Schutz-Gruppen.
- Darauf aufbauend findet auch ein Ranking der Service-Schutz-Gruppen statt.
- Zuordnung der Service zu den jeweiligen Service-Schutz Gruppen (Gruppierung der Service).
- Festlegung der Security Policies für die Border FW Sicherheits-Komponenten.
- Festlegung der Security Policies für IaaS.
- Festlegung der Security Policies für PaaS.
- Zusammenfassung von Security Policies in sogenannte Security Policy Gruppen.
- Zuordnung der jeweiligen Security Policy Gruppen zu den jeweiligen Service-Schutz-Gruppen.
- Eine Zuordnung von einzelnen Policies zu Service-Schutz-Gruppen oder auch zu einzelnen Service ist auch möglich.

Dies ist erforderlich, um die, für eine Ost-West-Kommunikation (innerhalb der Cloud-Umgebung) wie auch einer Nord-Süd-Kommunikation (z.B. Zugriff Client über Perimeterebene auf Anwendungen und Service) erforderlichen Policies anzuwenden.

- Die Kommunikation zwischen den Service-Schutz-Gruppen erfolgt grundsätzlich aus der „höherwertigeren Service-Schutz-Gruppe (vertrauenswürdiger)“ auf eine „niedrigere Service-Schutz-Gruppe (weniger vertrauenswürdig)“ oder zwischen gleichwertigen Service-Schutz-Gruppen bidirektional. Eine Kommunikation zwischen den Service-Schutz-Gruppen kann aus der „niedrigeren Service-Schutz-Gruppe (weniger vertrauenswürdig)“ auf eine „höherwertige Service-Schutz-Gruppe (vertrauenswürdig)“ erfolgen, wenn Isolierungs- und Prüfmechanismen in den Policies der Service-Schutz-Gruppen definiert sind.
- Festlegung der Isolierungs-Mechanismen pro Gruppe. Hierbei wird auch beachtet, ob es sich um einen reinen IaaS Service oder um einen PaaS Service handelt, da dies die Isolierungs-Möglichkeiten beeinflusst.
- Administration und infrastrukturelle Querschnittsdienste sind von Services zu trennen. Dies ist bei der Gruppendefinition zu beachten.
- Für jeden Mandanten werden für die Ebene 3 pro Service Schutz-Gruppe eigene infrastrukturelle und fachliche Querschnittsdienste eingerichtet. Der Nutzung von mandantenübergreifenden Querschnittsdiensten kann zugestimmt werden, wenn dies mit entsprechender Begründung beantragt wird. Hierfür ist der Nachweis einer sicheren Isolierung (fachlich, administrativ und infrastrukturell) der Mandanten durch den DL zu erbringen.

3.4 Konzeptioneller Aufbau der Ebenen

Ebene 1: Client-Zugriffsebene (User)

Ebene 1 stellt die Zugriffsebene dar, in der jeder Mandant eine eigene Client-Infrastruktur hat. Der Zugriff des Nutzers über den Client auf die Service erfolgt über die Anbindung an Ebene 2. Diese Ebene wird hier nicht betrachtet, so lange sie nicht in Form von Clientvirtualisierung innerhalb des SDDC auf Ebene 3 bereitgestellt wird.

Ebene 2: Sicherheitsinfrastruktur (Perimeterschutz)

Diese Ebene fungiert mit der Einführung von SDDC als Border-FW, d.h. die Netz-Segmentierung in der Ebene 3, DMZ für die Services, werden per SDN-Edge-FW zur Verfügung gestellt.

Ferner stellt die Ebene 2 Funktionen wie Hardware-Loadbalancer für die SDDC Umgebung zur Verfügung, insbesondere für User- und Service-Zugriffe bei HA (High Availibilty) Szenarien zwischen synchronen aber auch georedundanten Rechenzentren.

Die Ebene 2 führt ferner die ersten Identitätsprüfungen (AAA) der zugreifenden User und Services in Verbindung mit dem Querschnittsdienst Identity-Access-Management (IAM) durch.

Für die Ebene 2 sind Security Gruppen und Security Policies zu definieren.

Die Ebene 2 wird nicht mittels Infrastruktur-Komponenten der SDDC-Lösung bereitgestellt.

Ebene 3: Anwendungen und Datenhaltung

In Ebene 3 werden Services sowie Anwendungen bereitgestellt. Eine gemeinsame mandantenübergreifende Nutzung von Services und Anwendungen ist grundsätzlich möglich. Die bereitgestellten Service und Anwendungen untergliedern sich in Applikation, Datenhaltung, infrastrukturelle und fachliche Querschnittsdienste und Client Funktionen wie Terminalserver/Virtual-Desktop-Infrastruktur (VDI).

Die Service und Anwendungen müssen Service-Schutz-Gruppen zugeordnet werden. Die Kommunikation und der Schutz der Service und Anwendungen findet mittels Security Policies und Security Policy Gruppen der Ebene 2 oder 4 statt.

Korrespondierende Sicherheitsfunktionen der Anwendung und Querschnittdienste bietet in der Ebene 3 zum Beispiel ein zentrales IAM mit der Rechtevergabe für die Anwendungen oder eine DB-Firewall mit FW-Mechanismen. Weitere Bespiele sind Betriebssystem- und Web-Server Härtung oder Serverless Services.

Jeder Service und jede Anwendung muss explizit entsprechend seiner Gruppen-Zuordnung konfiguriert werden.

Service und Anwendungen, die mandantenübergreifend oder mit Dritten kommunizieren, müssen zwingend mittels API-Management/Security isoliert werden.

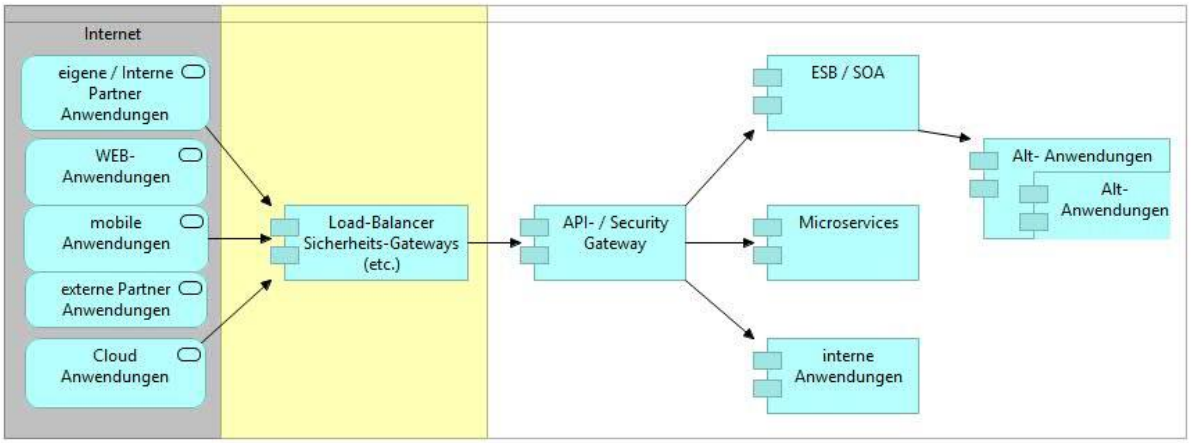

Abbildung 23: Prinzipielle Darstellung Management

Alle Service werden per Infrastruktur-Management oder Plattform-Management automatisiert und orchestriert verwaltet und installiert. Sie werden ggf. in Container gekapselt oder als nativer Micro-Service (µS) mittels zentraler PaaS Steuerungs-SW administriert.

Container und µS basierte Services müssen immer als SW Artefakt dem DL zur Verfügung gestellt werden, um ihm die Option einer (Source) Analyse zu bieten. Ferner ermöglicht diese Vorgabe die Härtung der Service Bestandteile (z.B. OS, Web-Server etc…).

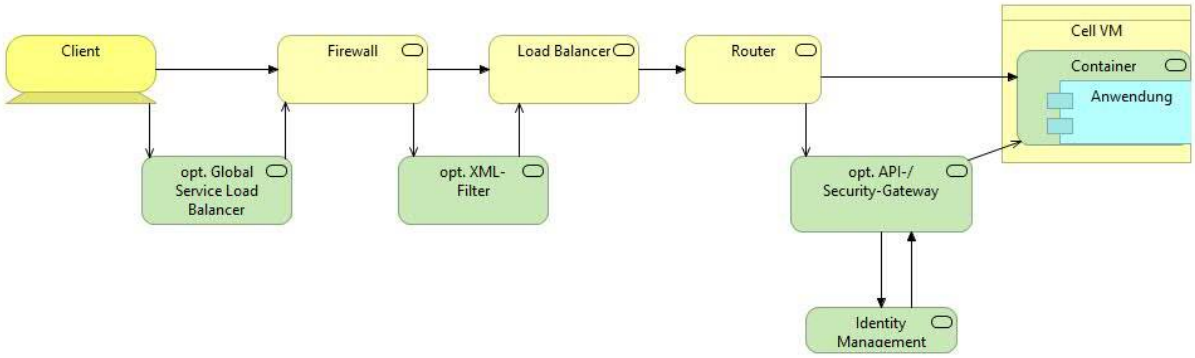

Abbildung 24:Darstellung prinzipielle Möglichkeit zur Härtung von Services

Ebene 4: IT-Infrastruktur

Hypervisor Cluster in der Ebene 4 stellen Software definierte Server (VMs) und Storage (vSAN) als Ressourcen für die Ebene 3 zur Verfügung.

In der Ebene 4 befinden sich die Hypervisorkomponenten, die z.B. für die SDN Edge, die SDN FW mit Third Party Sicherheits-Komponenten und für das API Management als Grundlage fungieren können.

Die SDN Edge-Komponenten stellen die SDN-Funktionalität her und die Verbindung der SDDC-Umgebung zum physikalischen Netzwerk sicher. Hierüber erfolgt auch die Anbindung bzw. der Zugriff auf externe Netze über die klassische Perimeterebene. Über diese SDN-Edge Komponenten werden auch die Verbindungen über externe bzw. nicht virtualisierte / softwaredefinierte Ressourcen/Service (z.B. externer Storage, Appliance für Datenbanken) sichergestellt.

Die SDN-Edge-Komponente bietet für die Ebene 3 Netzfunktionalitäten u.a. Netzsegmentierung, Loadbalancing, NAT oder auch Routing an.

Third Party Security Komponenten, in verteilten SDN-Firewall integriert, bieten Sicherheits-Funktionen wie Protokoll-Typ Prüfung an.

Viren Scanner Funktionen prüfen im Datenflow. Dieser Service wird auf explizit bereitgestellten und skalierbaren VMs installiert.

Als zusätzliche Sicherheits-Komponente muss in der SDN Edge Umgebung oder im Bereich der verteilten Firewall ein integriertes API-Management mit API-Security Funktionen für die Ebene 3 eingebunden werden.

Ebenso befinden sich hier Querschnittsdienste wie DNS, NTP, DHCP, PSC (Plattform Service Controller), software-defined-Management-Komponenten für die Automatisierung, Orchestrierung, Monitoring und Logging, Plattform-Steuerung.

Auch für die Ebene 4 sind Security Gruppen und Security Policies zu definieren.

3.5 Management im SDDC

Die Management-Umgebung ist von IaaS-, PaaS- und SaaS Komponenten sowie von den Services physikalisch getrennt aufzubauen.

Die Management-Umgebung wird auf ein eigenes Netz-Segment aufgebaut. Hier können die beschriebenen Sicherheitskomponenten getrennt zur Isolierung genutzt werden. Es beinhaltet Tools zur Erstellung der Automatisierung, Software für Überwachung und Steuerung sowie für Protokollierung. Der Management-Hypervisor-Cluster beinhaltet eigene Hosts für die beschriebenen Managementfunktionalitäten.

Die Management-Umgebung nutzt externe Querschnittsdienste wie Key-Management, Privileged Account Management (PAM), Verzeichnisdienst und Fileservice. Die Querschnittsdienste benötigen u.U. eigene Hardware oder Software (u.a. für PAM, Key- Management, Fileservice, FW, NTP, DNS, DHCP).

Der administrative Zugriff auf die Management-Umgebung erfolgt über Terminalserver/VDI (Admin- und Fernzugriff). Die personifizierte Authentifizierung des Administrators erfolgt darüber hinaus über PAM. Die Zugriffe werden protokolliert.

Die Kommunikation der Managementkomponenten mit der Payload[2]-Umgebung erfolgt zertifikatsbasiert. Es ist hierfür ein Key-Management erforderlich.

Bei einer SDDC Lösung mit zentralem Management inklusive einer zentralen Monitoring / Logging Funktionalität, muss eine entsprechende Isolierung über alle zu überwachenden Komponenten gewährleistet sein. Hierbei sind die Ebenen-Übergänge möglichst zu vermeiden, d.h. jede Ebene führt ein explizites Monitoring & Logging durch.

Die Querschnittsdienste werden über Firewall einerseits vom Management andererseits zu den Edge-Komponenten und Payload-Komponenten abgesichert.

2 Payload-Umgebung stellt die Umgebung der Nutzdaten dar.

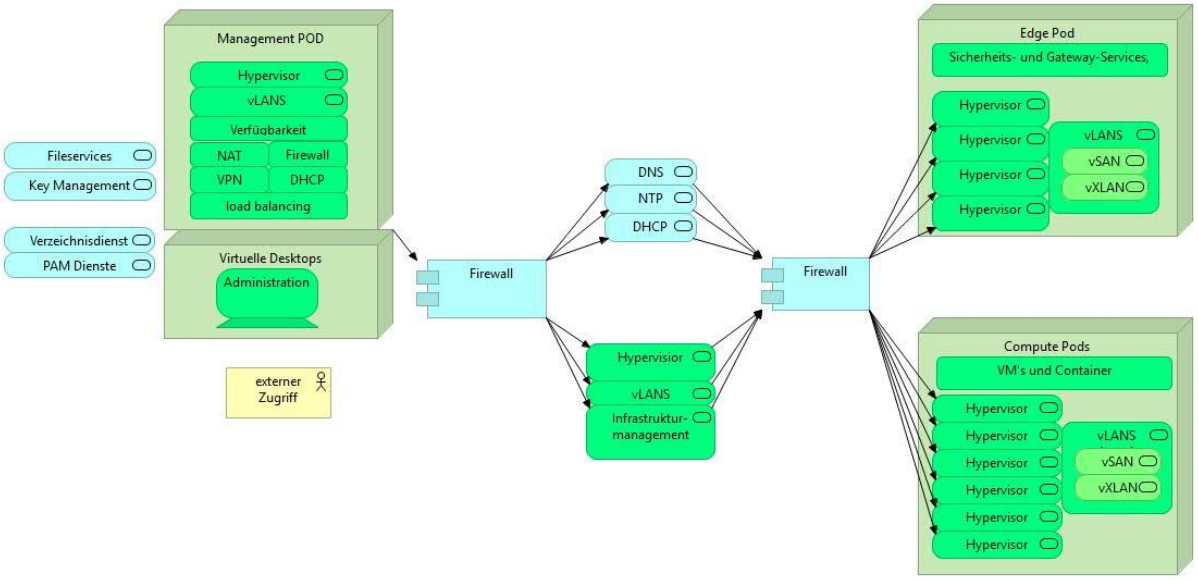

Abbildung 25: Beispiel - Logischer Aufbau eines Managemenst im SDDC

3.6 Prozesse und Rollen im SDDC

Mit Einführung von SDDC und den damit verbundenen Prozessen verändern sich Rollen und Zuständigkeiten stärker als im Bereich der klassischen Servervirtualisierung sowohl im Service- als auch im Infrastrukturbereich. Daher sind entsprechende Prozesse und Rollen festzulegen. Hier gibt es getrennte Organisationsstrukturen für den Infrastrukturbereich und dem Service-Team. Die Rollen sind sowohl für den Dienstleister als auch für den Mandanten zu definieren und festzulegen. Ebenfalls die Schnittstellen zwischen Dienstleister und Mandant.

Folgende Bereiche werden benötigt:

1. SDDC Infrastrukturservice-Team
2. SDDC Services-Team
3. SDDC Portfolio-Management-Team

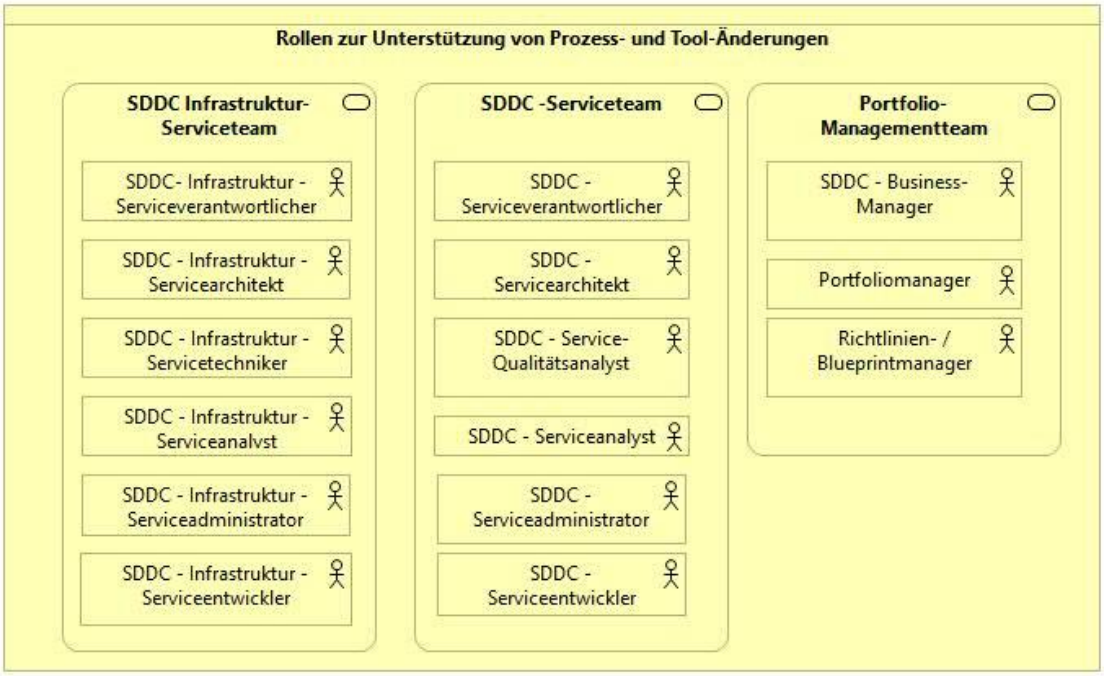

Abbildung 26: Beispiel für Rollen bei Nutzung SDDC

Ein Anbieter von SDDC-Service stellt ein Infrastruktur-Serviceteam bereit und in Teilen auch Rollen aus dem Serviceteam. Die jeweiligen Verantwortlichen bilden die Schnittstelle zwischen Infrastruktur-Team und Service-Team.

Infrastrukturservice-Team

Das Infrastrukturservice-Team benötigt Rollen u.a. als

- Verantwortlicher
- Architekt (Infrastrukturarchitekt)
- Techniker
- Analysten
- Administrator sowie
- Entwickler.

Das Infrastrukturservice-Team stellt Infrastruktur, Plattform und Software bereit. Das Infrastrukturservice-Team ist verantwortlich für die Ebenen 2, 3 und 4. In diesem Team werden die Sicherheitsrichtlinien umgesetzt und deren Einhaltung geprüft.

Service-Team

Das Service-Team benötigt Rollen u.a. als

- Verantwortlicher
- Architekt (Facharchitekt)
- QA (u.a. Qualitätssicherung, Reviews, Compliance-Prüfung)
- Analyst (u.a. überwacht Services, erstellt Reports, Kosten-Nutzen-Verhältnis)
- Administrator sowie
- Entwickler.

Der Mandant wird u.a. Rollen besetzen wie Service-Verantwortlicher, Service-Analyst und auch Service-Architekt. Der Service-Administrator setzt den Service um. Dies kann der Dienstleister sein, aber auch der Mandant selber.

Das Service-Team erstellt und verantwortet die fachlichen Service. Es stellt die Schnittstelle zur Fachlichkeit, zum Anforderer, Produktmanagement, Kundenmanagement, Prozesse sowie Service dar. Das Team nutzt die bereitgestellte Infrastruktur.

In diesem Team werden die Sicherheitsrichtlinien umgesetzt und deren Einhaltung geprüft.

Die Rollen werden sowohl durch den Dienstleister als auch durch den Mandanten wahrgenommen. Hierbei ist auf Funktionstrennung / „Segregation of Duites“ zu achten.

Portfolio-Management-Team

Das Portfolio-Management-Team benötigt folgende Rollen:

- Business-Manager
- Portfoliomanager
- Richtlinien-/Blueprint-Manager.

Hier sind Aufgaben des IT-Architekten, der IT-Sicherheit, der Geschäftsprozesse sowie Koordination verortet. Servicekataloge werden bereitgestellt. In diesem Team werden die Sicherheitsrichtlinien und Blueprints erstellt. Das Portfolio-Management-Team wird durch den Mandanten gestellt.

3.7 Mindestanforderungen

Die Mindestanforderungen an die unterschiedlichen Ebenen und Szenarien werden in

- Anlage 8: Ebene 1: Client – Zugriffsebene - SDDC
- Anlage 9: Ebene 2: Sicherheitsinfrastruktur (Perimeterschutz) - SDDC
- Anlage 10: Ebene 3: Anwendung und Datenhaltung (Service /App) - SDDC
- Anlage 11: Ebene 4: Infrastruktur - SDDC
- Anlage 12: Erweiterte Anforderungen an die Administration der Ebenen 1-4 - SDDC
- Anlage 13: Erläuterungen zur Referenzarchitektur an Hand von Beispielen - SDDC

beschrieben. Dabei werden zunächst die Gefährdungen aufgeführt. Anschließend werden die umzusetzenden Maßnahmen aufgeführt.

Anlage 8: Ebene 1: Client – Zugriffsebene - SDDC

Zunächst werden die Gefährdungen der Ebene 1 beschrieben, die durch eine Konsolidierung entstehen können. Darauf aufbauend werden die umzusetzenden Maßnahmen aufgeführt.

Gefährdungen

- Keine Gewährleistung eines homogenen Sicherheitsniveaus über alle Mandanten, da Gremienbeschlüsse des AK II – Innere Sicherheit- nur innerhalb des polizeilichen Informationsverbundes bindend und durchsetzbar sind. Somit ist ein Gefälle beim Sicherheitsniveau von Polizeien zu Dritten möglich.
- Infektion der Clients durch Verwendung von Wechselmedien über offene Schnittstellen am Client
- Zugriff der Clients auf unsichere Netze.
- Keine Überprüfung des Sicherheitsniveaus möglich.
- Kompromittierung durch eine Kopplung der Clients von mehreren Mandanten durch eine zentrale Administration dieser Clients.
- Kompromittierung durch eine Kopplung der Clients von mehreren Mandanten durch gemeinsame Nutzung (Konsolidierung) von fachlichen und infrastrukturellen Querschnittsdiensten.
- Administration mehrerer QS und Infrastrukturen durch einen Administrator.

Maßnahmen

- Pro Polizei-Client-Umgebung sind eigene Client-Querschnitts-Dienste wie AD/DNS usw. einzusetzen, Ausnahme: Eine Abweichung ist möglich, wenn der Dienstleister eine anderweitige sichere Trennung der Mandanten nachweisen kann.
- Client-Infrastruktur, die zentral gehostet wird, wird in der Ebene 3 betrachtet.
- Die fachliche Nutzung der Clients als User, Fachadministrator oder IT-Administrator in den unterschiedlichen Ebenen muss durch geeignete Maßnahmen abgesichert werden.

Anlage 9: Ebene 2: Sicherheitsinfrastruktur (Perimeterschutz) - SDDC

Hier ist zwischen der Perimeterebene und der Kommunikation zwischen den Services, die sich innerhalb der SDDC/SDN Umgebung befinden, zu unterscheiden.

Die klassische Perimeterebene sichert die SDDC Umgebungen und die „Außengrenze“ ab.

Gefährdungen

- Fehlkonfiguration der Sicherheitskomponenten beeinträchtigt alle Mandanten.
- Ausfall der Sicherheitskomponenten (Hardware) beeinträchtigt alle Mandanten.
- Kompromittierung durch fehlenden Trennungsmechanismus.
- Kopplung der Mandanten durch konzeptionelle Schwächen im Trennungsmechanismus.
- Fehler in der Komponente, die die logische Trennung durchführt.
- Kompromittierung durch eine Kopplung der Sicherheitskomponenten von mehreren Mandanten durch gemeinsame Nutzung (Konsolidierung) von fachlichen und infrastrukturellen Querschnittsdiensten.
- Sicherheitsinfrastruktur ist nicht hinreichend vor unbefugten Zugriff geschützt
- Fehlkonfiguration der Templates / Blueprints.
- Zugriff Unbefugter hat weitreichendere Folgen durch Konsolidierung der Management-Zentrale.
- Zugriff auf SDDC-Lösung über Perimeterebene auf existierende Schnittstellen.
- Ausfall durch DDoS.

Maßnahmen

- Die Trennung der einzelnen Sicherheitskomponenten von Polizeien zu Dritten erfolgt durch eine physikalische Trennung (fachlich, administrativ und infrastrukturell) oder einer vergleichbaren Isolierung (fachlich, administrativ und infrastrukturell).
- Für den Betrieb der Komponenten auf Hypervisor-Infrastruktur wird eine von den anderen Infrastrukturen getrennte, d.h. eigene Hypervisor-Infrastruktur für Ebene 2 benötigt.
- Umgebung(en) Dritter und Umgebung(en) Polizei sind getrennt über eigene LANs oder vergleichbare Schutzmaßnahmen an die Infrastruktur des Dienstleisters anzubinden.
- Prozess zur Erstellung der Blueprints erfolgt qualitätsgesichert 2-stufig inkl. Genehmigungsprozess für die Bereitstellung.
- Absicherung der Schnittstellen für den Zugriff aus der SDDC-Umgebung in die Ebene 2.
- Nutzung geprüfter Templates.
- Kommunikation zwischen polizeilichen Mandanten und Dritten erfolgt über eine PAP-Struktur – verbunden über SDN-Edge-zur klassischen Perimeterebene (Border-FW). (Border-FW als klassische Perimeterebene wird nur für den Zugang genutzt). Die Trennung der einzelnen Sicherheitskomponenten von Polizeien zu Dritten erfolgt über die Perimeter Ebene.
- Identitätsprüfung (AAA) der zugreifenden User und Services in Verbindung mit dem Querschnittsdienst IAM.
- Es sind Security Gruppen und Security Policies zu definieren.

Anlage 10: Ebene 3: Anwendungen und Datenhaltung (Service / App) - SDDC

Gefährdungen

- Kompromittieren durch fehlenden Trennungsmechanismus.
- Fehlkonfiguration der Anwendungs- und Datenhaltungskomponenten beeinträchtigt alle Mandanten.
- Kopplung der Mandanten durch konzeptionelle Schwächen im Trennungsmechanismus.
- Fehler in der Komponente die die logische Trennung durchführt.
- Kompromittieren durch eine Kopplung der Anwendungs- und Datenhaltungskomponenten von mehreren Mandanten durch eine zentrale Administration der Anwendungs- und Datenhaltungskomponenten.
- Kompromittieren durch eine Kopplung der Anwendungs- und Datenhaltungskomponenten von mehreren Mandanten und Dritte durch gemeinsame Nutzung (Konsolidierung) von fachlichen und infrastrukturellen Querschnittsdiensten.
- Diebstahl oder Verfälschung von Nutzdaten.
- Nicht den gesetzlichen Vorgaben entsprechendes Löschen von Nutzdaten.
- Die Automatisierungskomponente verfügt über 2 Schnittstellen: zum User-Netz sowie zur Infrastruktur zum Durchreichen der Blueprints über alle Ebenen. Zudem greift der User über Self-Service-Portal auf Automatisierungskomponente zu.
- Höhere Gefährdung durch Fehlerkonfiguration, durch die mehr Komponenten betroffen sind.

Maßnahmen

- Kommunikationen zwischen zwei Services sind explizit mittels software-definierten Netzwerk-Tools zu realisieren. Es wird ein logisches Netz pro Service-Kommunikation definiert, welches keinen Übergang zu anderen Netzen ermöglicht.
- Wenn Polizeien ihre Infrastruktur bei einem Dienstleister gemeinsam nutzen, kann die polizeiliche mandantenübergreifende Kommunikation zwischen Service über Hypervisor-FW-Mechanismen erfolgen. Hierbei wird zwischen zwei Service explizit ein logisches Netz mittels software-definierten NW-Tools aufgebaut. Hierbei besteht keine Kommunikationsmöglichkeit mit anderen Netzen.
- Der Zugriff der Clients auf Service-Schutz-Gruppen sowie die Kommunikation zwischen Service-Schutz-Gruppen verschiedener Mandanten (Dritter) erfolgt über die Perimeterebene. Der Datenaustausch erfolgt immer über aktive Sicherheitskomponenten.
- Die Kommunikation zwischen Service-Schutz-Gruppen verschiedener polizeilicher Mandanten innerhalb der gemeinsam genutzten Infrastruktur eines Dienstleistes kann über Hypervisor-FW-Mechanismen erfolgen. Paketfilter des Hypervisor oder Third-Party-Komponenten für ALG Funktionalitäten können hierbei genutzt werden.
- Service-Schutz-Gruppen übergreifende Kommunikation von Anwendungen kann bei einer ausreichenden Isolierung auch über die Ebene 4 mittels SDN Komponenten erfolgen, d.h. der Sicherheitsinfrastruktur in der Ebene 4 (z.B. SDN-FW und Third-Party Sicherheits-Komponenten auf einem Hypervisor).
- Es ist bei der Kommunikation zwischen den Services ein White-Listing Ansatz umzusetzen, d.h. jede Verbindung ist explizit freizugeben.
- Prozess zur Erstellung der Blueprints erfolgt qualitätsgesichert 2-stufig inkl. Genehmigungs-prozess für die Bereitstellung. Es erfolgt die Nutzung geprüfter Templates.
- Verschlüsselung der VMs verhindert Zugriff auf Daten (Vertraulichkeit).
- Hostprofilemanagement (sobald Konfiguration des Hosts nicht dem Regelwerk entspricht, werden Maßnahmen ergriffen) – Überwachung eines SOLL-Zustands.

- Durch Microsegmentierung im Netzwerk können Gefährdungen besser begegnet werden (Ausbreitung Schadprogrammen, Missbrauch von Berechtigungen).
- Anwendungen/Services werden in DMZ(en) betrieben bzw. sind mittels SDN Mechanismen oder innerhalb SDDC eingesetzter Isolierungsmechanismen (Security Policies) getrennt.
- Es können VLAN bzw. VXLAN innerhalb der einzelnen Service-Schutz-Gruppen genutzt werden.
- Service, die Mandanten übergreifend oder mit Dritten kommunizieren, müssen zwingend mittels API-Management/Security isoliert werden.

Anlage 11: Ebene 4: IT-Infrastruktur - SDDC

Gefährdungen

- Kompromittieren durch fehlenden Trennungsmechanismus.
- Fehlkonfiguration der Storagekomponenten, Computenodes, Netze, infrastrukturellen Querschnittsdienste beeinträchtigt alle Mandanten.
- Ausfall der Storagekomponenten, Computenodes, Netze, infrastrukturellen Querschnittsdienste (Hardware) beeinträchtigt alle Mandanten.
- Kopplung der Mandanten durch konzeptionelle Schwächen im Trennungsmechanismus.
- Fehler in der Komponente die die logische Trennung durchführt.
- Kompromittieren durch eine Kopplung der Storagekomponenten, Computenodes, Netze, infrastrukturellen Querschnittsdienste von mehreren Mandanten durch eine zentrale Administration der Storagekomponenten, Computenodes, Netze, infrastrukturellen Querschnittsdienste.
- Kompromittieren durch eine Kopplung der Storagekomponenten, Computenodes, Netze, infrastrukturellen Querschnittsdienste von mehreren Mandanten durch gemeinsame Nutzung (Konsolidierung) von fachlichen und infrastrukturellen Querschnittsdiensten.
- Diebstahl oder Änderung von Nutzdaten.
- Kunden-Netzwerk, IP-/MAC-Spoofing, Man-in-the-Middle, Pooling von Ressourcen – d.h. Angreifer hat komplettes Netzwerk.

Maßnahmen

- Storagekomponenten, Computenodes, Netze, infrastrukturelle Querschnittsdienste sind pro Service-Schutz-Gruppe mittels SDN Mechanismen oder innerhalb SDDC eingesetzter Isolierungsmechanismen (Sercurity Policies) zu trennen.
- White-Listing der Services / Applikationen mittels SDN.
- Nutzung SDDC / Hypervisor Sicherheitskomponenten und Third-Party-Sicherheitskomponenten.
- Compute Nodes werden auf getrennten Hypervisor Clustern abgebildet.
- Nutzung qualitätsgesicherter Blueprints, die einem Genehmigungsprozess für die Bereitstellung unterliegen.
- Auf Grund der Netzwerkinfrastruktur gibt es keinen Broadcast-Traffic außerhalb eines Clusters.
- Trennung der Administratoren oder 4-Augen-Prinzip.

Anlage 12: Erweiterte Anforderungen an die Administration der Ebenen 1-4 - SDDC

Alle Ebenen

- Der Zugriff auf die Infrastruktur muss in einem Rechte-und-Rollen-Attribute-Konzept geregelt sein und muss eine Zwei-Faktor-Authentisierung vorsehen. Hierbei fungieren die Sicherheitskomponeten als Policy Enforcement Point (PEP) und prüfen mittels dem zentrale Access-Management als Policy Decision Point (PDP), ob das zugreifende Objekt (Service oder User) seine Identität nachgewiesen und entsprechende Rechte hat.
- Die Wirksamkeit der Maßnahmen, um die Sicherheitsinfrastruktur vor unbefugten Zugriffen abzusichern, sollte zyklisch durch einen Penetrationstest überprüft werden. Gefundene Schwachstellen sollten zeitnah behoben werden.
- Eine mandantenübergreifende Administration durch den Dienstleister ist grds. möglich. Natürlich hat hierbei der Zugriff über personifizierte Accounts zu erfolgen. Es ist eine Trennung root und anderen privilegierten Accounts sowie eine sichere Protokollierung der Zugriffe (Nachvollziehbarkeit) sicherzustellen.
- Der Verbindungsaufbau erfolgt nur von den Admin-Clients in die Schutzzone(n), nicht umgekehrt.
- Der Admin-Zugriff auf die Management-Umgebung erfolgt mittels PAM (Privileged Account-Management) und mittels Terminalserver/VDI über eine aktive Sicherheitskomponente. Der administrative Zugriff auf die Management-Komponenten ist zu überwachen sowie zu protokollieren.

Nur Ebene 1

- - - O H N E - -

Nur Ebene 2

- Die Administration der Ebene 2 erfolgt ausschließlich durch den Dienstleister.

Nur Ebene 3

- Die Administration der Ebene 3 erfolgt ausschließlich durch den Dienstleister unter Beachtung folgender Punkte:
    - Die Nutzung/Verwaltung von Services über DMZen durch ein Tool wird zugestimmt, wenn diese durch den Dienstleiter begründet beantragt werden. Hierfür ist der Nachweis einer vergleichbaren Isolierung (fachlich, administrativ und infrastrukturell) der Mandanten/Service zu erbringen.
    - Wenn ein SDDC /SDN Lösung mit einem zentralen Management für alle Komponenten der Ebene 2-4 angedacht ist, muss die Management-Umgebung durch Sicherheitskomponenten geschützt werden, sowohl Richtung Admin-Zugriff als auch Richtung der Service-Infrastruktur.
- Der Kunden-Administrations-Zugriff erfolgt mittels Token (föderative Identitäten-Management (IDM)) über User-Daten-Netz mit Zwei-Faktor-Authentifizierung und Prüfung der Identität und Rechte.

Nur Ebene 4

- Die Administration der Ebene 4 erfolgt ausschließlich durch den Dienstleister.

Anlage 13: Erläuterungen zur Referenzarchitektur an Hand von Beispielen - SDDC

SharedApplikation im Bereich der polizeilichen Infrastruktur

Bei einer SDDC/SDN Lösung kann für die polizeilichen Mandanten und für Schutzzone SharedApplikation (ShA) eine Ebene 4 Umgebung genutzt werden. Die Kommunikation mit der SZ ShA ist hierbei aber über die Perimeter Ebene abzusichern.

Zukünftig ergibt sich durch die Verwendung von einer Plattform Steuerungs-SW-Komponente die Option, administrative Aufwände für die Zurverfügungstellung von Services zu minimieren.

Damit besteht die Möglichkeit in der Ebene 3 die Trennung / Isolierung der einzelnen Services / Applikation zu erhöhen.

Fall 4: In diesem Beispiel geht die Konsolidierung noch einen Schritt weiter. Hier erfolgt die Mandantentrennung innerhalb der Anwendung – die Anwendung muss dies unterstützen, z.B. über gut implementierte Rechte- und Rollenkonzepte. Getrennte Datenhaltung oder gemeinsame DB sind auch hier möglich, wenn dies durch die Anwendung unterstützt wird.

Mit der Verwendung von einer Plattform Steuerungs-SW-Komponente können die Isolierungs-Risiken des Fall-Beispiels 3 vermieden werden.

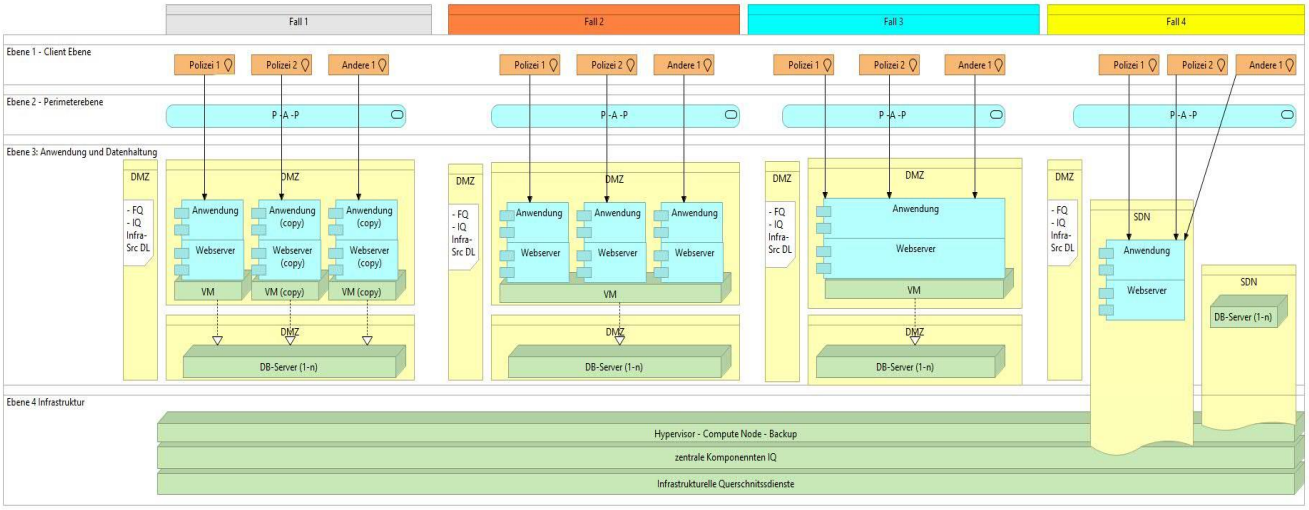

Abbildung 27: logische Abbildung einer möglichen Shared Applikation (Fall 3) auf Ebene 4