DEUTSCHE VERWALTUNGSCLOUD
EIN PRODUKT DES IT-PLANUNGSRATS

Detailstandard 01: Zonenmodell am (DVC) Cloud-Standort

Version 2.0 (28.12.2025)

Inhaltsverzeichnis

Zusammenfassung

Dieser Detailstandard regelt das "Zonenmodell am Cloud-Standort" (für Cloud-Service-Anbieter der DVC im Sinne von Plattformbetreibern und Softwarebetreibern, sofern letztere eigene Cloud-Standorte unterhalten). Dieser Detailstandard beschreibt ein am IT-Grundschutz ausgerichtetes, einheitliches Zonenmodell zur Umsetzung in allen Cloud Standorten der DVC.

Disclaimer

Die Vorgaben und Richtlinien des BSI haben in der aktuellen föderalen Aufstellung eine unterschiedlich starke Auswirkung für Einrichtungen von Bund, Ländern und Kommunen. Sie erzielen unterschiedlich starke Wirkung, d.h. Bundesbehörden und deren IT-Dienstleister müssen sich dran halten, Länder und Kommunen haben hingegen eigene Regelwerke, die auf jeden Fall ebenfalls zu beachten sind. Daher versucht die DVC mit diesem Detailstandard, einen allgemeingültigen Einstieg in die Thematik zu finden. Die maximalen Vorgaben sind in BSI-Standard 200-2 formuliert, z.B. Differenzierung bei der Zonierung: vgl. BSI-Standard 200-2, S. 132, Zonenkonzept beim Cloud Computing

→ Dennoch wollen wir hier in der DVC eine einheitliche Sicht auf das Zonenmodell von Cloud Standorten etablieren!

Anforderung

Ein **Cloud-Standort in der DVC** ist grundlegend immer über die Verwaltungsnetze der öffentlichen Verwaltung zugänglich; er kann auch über das Internet zugänglich gemacht werden. Für die Anbindung an die Verwaltungsnetze der öffentlichen Verwaltung gehen wir aktuell von einer Kopplung über das NdB-VN (Netzwerk des Bundes - Verbindungsnetz) aus, welche sukzessive in eine DVC-Netzstruktur entwickelt werden kann. In diesem Fall gelten die Anschlussbedingungen der BDBOS; weitere Vorgaben zur Qualität werden für die DVC nicht gemacht. Die **Anbindung an das NdB-VN ist verpflichtend** für Cloud-Standorte der DVC. Die **Anbindung an das Internet** ist optional. Die Qualität der Internet-Anbindung ist in Detailstandard #2 gesondert geregelt.

Cloud-Services der DVC sind entsprechend des Zugangsmodells (Öffentliches Internet versus Interne Verwaltungsnetze) in Zonen zu positionieren. Wir unterscheiden dabei eine **(externe) Zone für DVC-Services (gegenüber dem Internet)** und eine **(interne) Zone für DVC-Services (gegenüber den Verwaltungsnetzen)**.

Innerhalb von DVC-Cloud-Services sind **einzelne Anwendungen klar auf die (externe) Zone für DVC-Services (gegenüber dem Internet) und die (interne) Zone für DVC-Services (gegenüber den Verwaltungsnetzen) zu verteilen. Ein Zonen-übergreifender Mischbetrieb einer Anwendung ist nicht zulässig.** Einzelne Anwendungen können dabei schon auf eine der beiden Zonen verteilt sein, für Anwendungs-übergreifende Zugriffe zwischen den Zonen ist zu gewährleisten, dass Zugriffe immer nur von der "sicheren" (interne) in die "unsichere" (externe) Zone erlaubt sind. Beide Zonen werden durch **interne Management-Systeme** durch den Cloud-Service-Anbieter administriert. **Diese internen Management-Systemen müssen nicht für die beiden vorgenannten Zonen separiert werden.** Weitere Details regelt Detailstandard #28.

Auf die Cloud-Services wird nur über die Zugangswege (Internet und Verwaltungsnetze) zugegriffen. Dabei ist **zwischen Nutzer-Zugang für die Konsumierung der Cloud-Services und administrativem Zugang für die Verwaltung der Cloud-Services durch den Cloud-Service-Kunden und ihre Endnutzer** zu unterscheiden für beide Zugangswege (Internet und Verwaltungsnetze).

Der **Zugang** der Nutzenden (**"Frontend"**) von (i.d.R) Webinterfaces der Cloud-Services sowie für gemäß Rollen- und Rechte innerhalb der Cloud-Services fachlich Administrierende (Priviligierte Nutzer) muss **jeweils über eine eigene DMZ (De-Militarisierte Zone)** geführt werden. Dies **separat zu administrativem Zugang ("Backend")** zur Konstituierung & Verwaltung der Services (CRUD; Create-Read-Update-Delete), der über einen **gesonderten Zugangsweg zu führen** ist. Dieser wird in der Regel nicht "direkt" in die (interne oder externe) Zone für DVC-Services ausgeprägt sein, sondern an Verwaltungssysteme der Cloud-Standorte "andocken", die in den Management-Systemen verortet sind. Für den **Frontend-Zugang der Nutzenden & Fach-Administratoren regelt dies der Detailstandard #48 für beide Zugangswege (Internet und Verwaltungsnetze)** grundsätzlich. Für den Backend-Zugang der technischen Administration regelt dies für die Verwaltungsnetze der Detailstandard #49. Backend-Zugang über das Internet sollte in der DVC die Ausnahme sein. Sollte es erforderlich sein, Backend-Zugang über das Internet zu gewähren, müssen die Cloud-Service-Anbieter entsprechend "geeignete Absicherungsmechanismen" (z.B. VPN-Zugang) bereitstellen.

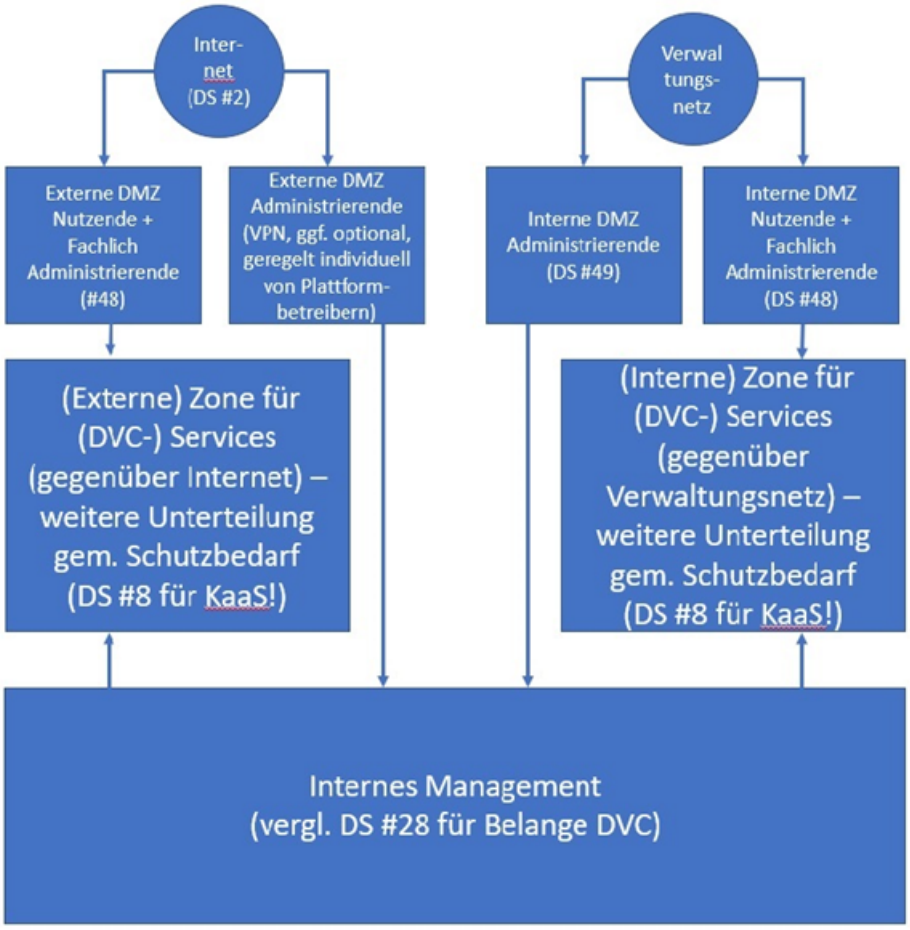

Abbildung 1: DVC-Zonenmodells der Cloud-Standorte

Abbildung 1: Blaupause des einheitlichen DVC-Zonenmodells der Cloud-Standorte

Aufbauend auf dieser Grundstruktur muss nun jeder Cloud-Service-Anbieter entscheiden, wie er die beiden Zonen für die DVC-Services weiter untergliedert in Bezug auf die Anforderungen des BSI nach "Zonentrennung" und "Schutzbedarfsklassen".

A - BSI Zonenmodell

Das Zonenmodell des BSI sieht eine Unterteilung in drei Hauptzonen vor (vgl. Abbildung 1).

Webzone:
Die Web-Zone wird zur Bereitstellung von Application-Level-Gateway bzw. Web-Proxy genutzt.

Anwendungszone:
Die Anwendungs-Zone wird zur Bereitstellung von Applikationsservern genutzt.

Datenbankzone:
Die Datenbank-Zone wird zur Bereitstellung von Datenbankmanagementsystemen genutzt.

Die **Trennung der Zonen kann BSI-konform sowohl physisch als auch virtuell erfolgen**, wenn dies sicherheitstechnisch auf gleichwertigem Niveau erreichbar ist. Die Zonen werden entsprechend den **Einschätzungen der Cloud-Standorte in Betrieb*** genommen. Es besteht keine Verpflichtung, alle Zonen in allen Fällen auszuprägen. Sofern beispielsweise eine Anwendung vollständig containerisiert ist, kann die Webzone durch vorgelagerte Systeme (z.B. eine P-A-P-Struktur des Betreibers) abgebildet werden und Anwendungszone und Datenbankzone können zusammengelegt werden.

Standort-spezifische und mit den Vorgaben des BSI konforme Abweichungen sind möglich. Die Zugangswege von einer Zone in eine andere sind den in der Abbildung aufgeführten Beschränkungen unterworfen.

B - Schutzbedarfsanalyse

Der Betrieb eines Services muss eine Schutzbedarfsanalyse seiner Daten vorausgehen. Systeme sind gemäß Schutzbedarf voneinander zu separieren. Inwieweit dies eigene physische Strukturen erfordert, obliegt der Einschätzung des Cloud-Service-Anbieters

Standardisierung

Aus den Vorgaben ergeben sich folgende Detailanforderungen:

Grundlegende Feststellungen (Umsetzung Beispielbild)

ID	Rolle	Modal-verb	Detailanforderung
DS_01_A001	a) DVC-Plattformbetreiber (für eigene Cloud-Standort und auch als Cloud Integrator gegenüber Cloud-Standorten von Cloud Service Lieferanten) b) DVC-Softwarebetreiber (für eigene Cloud-Standort und auch als Cloud Integrator gegenüber Cloud-Standorten von Cloud Service Lieferanten)	MUSS	Der Cloud-Standort MUSS eine Anbindung an Verwaltungsnetze via NdB-VN haben. Der Cloud-Standort muss dazu die Anschlussbedingungen der BDBOS umsetzen; die Einhaltung eines weiteren Detailstandards ist nicht erforderlich
DS_01_A002	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	KANN	Der Cloud-Standort KANN eine Anbindung an das Internet haben

Fortsetzung auf nächster Seite

Fortsetzung von vorheriger Seite

ID	Rolle	Modal-verb	Detailanforderung
DS_01_A003	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	SOLL	Der Cloud-Standort SOLLTE für die Qualität der Internet-Anbindung Detailstandard #2 adaptieren.
DS_01_A004	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	MUSS	Der Cloud-Standort MUSS unabhängig vom Zugangsweg (Internet/Verwaltungsnetze) den Zugriff für Nutzende und Fachlich Administrierende eines Cloud Service (“Frontend”) vom Zugriff für die technische Verwaltung und Administration des Service (“Backend”) trennen über eigene DMZ-Strukturen
DS_01_A005	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	SOLL	Der Cloud-Standort SOLL unabhängig vom Zugangsweg (Internet/Verwaltungsnetze) den Zugriff für Nutzende und Fachlich Administrierende von Anwendungen eines DVC Cloud Service (“Frontend”) den Detailstandard #48 umsetzen.
DS_01_A006	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	SOLL	Der Cloud-Standort SOLL für den Zugangsweg Verwaltungsnetze den Zugriff für die technische Verwaltung und Administration des Service (“Backend”) den Detailstandard #49 umsetzen.
DS_01_A007	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	KANN	Der Cloud-Standort KANN für den Zugangsweg Internet den Zugriff für die technische Verwaltung und Administration des Service (“Backend”) über geeignete eigene Maßnahmen umsetzen nach Möglichkeit analog der Vorgaben von Detailstandard #49. Beispiel / Erläuterung **Zu “Service Konsumenten / Nutzenden”:** Der Fokus des aus der öffentlichen Verwaltung konsumierenden Service Nutzenden ist üblicherweise sicherheitsseitig auf den behördlichen Verwaltungsnetzen (Primärfokus) und nur bei geringem Schutzbedarf und besonderem Grund über das Public Internet angedacht. Natürlich ließe sich ggf per VPN-Zugang auch eine Lösung herstellen, welche sicherheitsseitig der nativen Internetvariante immer eindeutig überlegen ist. **Zu ” Fachlich administrierende und technisch Administrierende”** Jene sollten ebenso aus den behördlichen Verwaltungsnetzen und nicht nativ aus dem public Internet zugreifen aufgrund des unnötigen, erhöhten Angriffsrisikos. Auch hier sollte ein besonderer triftiger Grund vorliegen, warum man nicht von innen vom Behördennetz zugreifen kann. Auch hier wäre ggf. eine VPN Lösung dem nativen Internetzugriff definitiv immer vorzuziehen.

Fortsetzung auf nächster Seite

Fortsetzung von vorheriger Seite

ID	Rolle	Modal-verb	Detailanforderung
DS_01_A008	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	MUSS	Der Cloud-Standort MUSS abhängig vom Zugangsweg (Internet/Verwaltungsnetze) getrennte Zonen/Bereiche für die Bereitstellung Cloud-Services etablieren. Wir unterscheiden zwischen der ‘ “Internen” Zone für Anwendungen von DVC Cloud-Services mit Zugang über Verwaltungsnetze’ und der ’ “externen” Zone für Anwendungen von DVC Cloud-Services mit Zugang über das Internet.
DS_01_A009	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	SOLL	Der Cloud-Standort SOLLTE bei der die Nutzung von Kubernetes in der ‘ “Internen” Zone für Anwendungen von DVC Cloud-Services und der’“externen” Zone Anwendungen von für DVC Cloud-Services den Detailstandard #8 adaptieren.
DS_01_A010	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	MUSS	Der Cloud Standort MUSS seine Management-Systeme von den vorgenannten DMZ-Strukturen und den Zonen für Cloud-Services separieren
DS_01_A011	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	KANN	Der Cloud Standort KANN seine Management-Systeme ebenfalls zwischen “Internen” (zu Verwaltungsnetzen zeigenden) Management-Systemen und “externen” (zum Internet zeigenden) Management-Systemen separieren
DS_01_A012	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	SOLLTE	Der Cloud-Standort SOLLTE zur Detaillierung der Management-Systeme [Detailstandard #28] beachten.

Erweiterte Festlegungen (BSI-Bezug)

ID	Rolle	Modal-verb	Detailanforderung
DS_01_A050	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	MUSS	Der Cloud-Standort MUSS sicherstellen, dass die weiterführende Segmentierung nach Zonen gemäß der BSI-Vorgaben (Web - Anwendung - Datenbank) nicht durch die Management-Kommunikation unterlaufen werden kann. Eine Überbrückung von Segmenten MUSS ausgeschlossen werden.
DS_01_A051	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	SOLL	Die Trennung zwischen den 3 BSI Zonen (Web - Anwendung - Datenbank) SOLL physisch erfolgen.
DS_01_A052	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	KANN	Die Trennung zwischen den 3 BSI Zonen (Web - Anwendung - Datenbank) KANN mittels virtueller Systeme umgesetzt werden, wenn die Sicherheitsanforderungen gleichwertig einer physischen Trennung realisiert werden.
DS_01_A053	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	MUSS	Eine Netztrennung zwischen Zonen MUSS mittels Firewalls mindestens bis zum Layer 4 erfolgen.

Fortsetzung auf nächster Seite

Fortsetzung von vorheriger Seite

ID	Rolle	Modal-verb	Detailanforderung
DS_01_A054	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	MUSS	Die Firewalls für Netztrennung MÜSSEN ausreichend dimensioniert werden, damit Lastspitzen und eine notwendige Skalierung abgesichert ist.
DS_01_A055	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	MUSS	Zonenübergänge sind mittels zweier beidseitiger Paketfilter im Cluster auszulegen.
DS_01_A056	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	MUSS	Als Standard wird nur der Zugriff aus einer sicheren in eine unsichere Zone unterstützt. Ausnahmen muss der Cloud-Standort im Sinne einer (Eigen-)Risikoübernahme individuell für sich freigeben. Es besteht kein Anspruch auf Umsetzung. Beispiel / Klarstellung Zur "Risikoübernahme": Da dies eine Normabweichung darstellt, sollte dieses Risiko ausdrücklich transparent gemacht werden (nicht nur Risiko still tragen), die aufgewendeten Mitigationsmaßnahmen zur Risikominimierung dokumentiert und die Anwendung an sich möglichst vermieden werden. Es gibt aber in der behördlichen Praxis durchaus solche Fälle. Tlw. gibt es mögliche Risikominimierungen durch Application Layer Gateways, Web Application Firewallsysteme, Pre-Authentication, usw.
DS_01_A057	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	MUSS	Folgende Kommunikationsregeln MÜSSEN beachtet werden:
DS_01_A058	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	MUSS	Kommunikationsverbindungen MÜSSEN ausschließlich mittels Whitelisting explizit freigegeben werden.
DS_01_A059	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	SOLL	Storage SOLLTE netztechnisch separiert werden.
DS_01_A060	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	KANN	Storage KANN über getrennte Netze zentral für mehrere Zonen bereitgestellt werden.
DS_01_A061	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	KANN	Die **unterschiedlichen Zonen** sind weiter **entsprechend unterschiedlichen Schutzbedarfen zu segmentieren**. Eine entsprechend Umsetzung im Bedarfsfall wird ausdrücklich empfohlen.
DS_01_A062	a) DVC-Plattformbetreiber b) DVC-Softwarebetreiber	MUSS	**"Schutzbedarf"** MUSS vom Cloud-Standort im **Konzept des hauseigenen Zonenmodells** berücksichtigt werden und im Sinne einer Transparenzpflicht dem Konsumenten (ggf. auf Verlagen) dargestellt wird.

DISCLAIMER

Hinweis: Bei dem Sprachgebrauch hier handelt es sich um "DVC-seitige Mindeststandards" und nicht um allgemeine Mindeststandards des BSI (bspw. gem. BSI Gesetz) oder andere Normierungsgruppen. Es wird davon ausgegangen, dass bei der Umsetzung eines QMS (ISO:9001) respektive ISMS (ISO:27001) respektive bei der Entwicklung von C5-konformen Services oder einer Zertifizierung nach IT Grundschutz die meisten Themen an einem Cloud-Standort ohnehin umgesetzt sind.

Referenzdokumente

Dieser Abschnitt führt alle für die Bearbeitung und das Verständnis des Produktes erforderlichen Dokumente an, dies schliesst BSI-Grundschutz-Bausteine als auch Blaupausen mit ein. Die Dokumente sollten hinsichtlich ihrer Verwendung (intern, extern) unterschieden werden. Über die referenzierten Dokumente sind folgende Informationen zu halten: Bezeichnung, Identifikation mit Versionsangabe und Art der Verwendung (z. B. Quelle, weiterführende Literatur, usw.)

Kapitel	Seite	Dokument	Version	Ablageort (Link)
(n/a)	132ff	IT-Grundschutz Kompendium	2023	IT-Grundschutz-Kompendium
(n/a)	(n/a)	IT Grundschutz Methodik	2023	IT Grundschutz Methodik

Abbildungsverzeichnis

Abkürzungsverzeichnis

Abkürzung	Bezeichnung
BSI	Bundesamt für Sicherheit in der Informationstechnologie
DVC	Deutsche Verwaltungs-Cloud
ISMS	Information Security Management System
NdB	Netzwerk des Bundes
NdB-VN	Netzwerk des Bundes - Verbindungs-Netz
P-A-P	Paketfilter - Application Level Gateway - Paketfilter
QMS	Qualitäts Management System