DEUTSCHE VERWALTUNGSCLOUD
EIN PRODUKT DES IT-PLANUNGSRATS

Detailstandard 02: Netzanbindung am Internetzugang

Version 2.0 (28.12.2025)

Inhaltsverzeichnis

Zusammenfassung

Dieser Detailstandard regelt die "Netzanbindung am Internetzugang" (eines "Cloud-Standortes") für die DVC (für Cloud-Service-Anbieter der DVC im Sinne von Plattformbetreibern und Softwarebetreibern, sofern letztere eigene Cloud-Standorte unterhalten). Der Detailstandard „Netzanbindung für den Internetzugang" beschreibt ergänzend zum Detailstandard #01 („Zonenmodell am (DVC) Cloud Standort") die qualitativen und fachlichen Anforderungen, die bei der Ausgestaltung der Internet-Anbindung beachtet werden müssen.

Disclaimer

Die u.a. Grafik für Schutzbedarf kann „normal" angewendet werden (in Umsetzung IT-Grundschutz). Hinweise:

- Bei höherem Schutzbedarf und/oder VS-Anforderungen kommen dann weitere Zonen dazu
- Bei hohem Schutzbedarf würden ggf weitere Komponenten an Sicherheitssystemen (wie Integritätschecker etc.) dazu kommen

Anforderung

Gegenstand der Betrachtung ist der **Übergang vom (öffentlichen) Internet in die (lokale BSI) "Webzone" des Cloud-Standorts** im Kontext von **Detailstandard #01 („Zonenmodell am (DVC) Cloud Standort")**, sowie der von dort ausgehenden Paketfilter (Firewalls) gegenüber den angebotenen "DVC Services" in der "Externen Zone für (DVC-)Services gegenüber dem Internet".

Abbildung 1: P-A-P-Struktur gemäß IT-Grundschutz des BSI

Gemäß IT-Grundschutz des BSI ist eine **P-A-P-Struktur abzubilden** (vgl. Abbildung 1). Der P-A-P-Struktur vorgelagert sollte möglichst durch den oder die genutzten Internet-Service-Provider (ISP) ein Dienst zur **Angriffserkennung und -abwehr** ("Intrusion Detection System"/IDS und/oder "Intrusion Prevention System"/IPS) etabliert werden, insbesondere für den Schutz vor (D)DoS-Angriffen externer Akteure. Zusätzliche sind weitere "**assozierte Sicherheitssysteme**" angenommen (z.B. ein SIEM-System, wie im Bereich "Standardisierung" ausgeführt.

Der Cloud-Standort selbst ist durch eine **redundante Netzanbindung** mit mindestens zwei physischen Leitungen an das Internet angebunden. Die beiden **Paketfilter** dienen auch als **Firewalls**. Das **Application Level Gateway** (synonym mit der "**Webzone**" in Abbildung 1 enthält Komponenten wie beispielsweise eine Web Application Firewall (WAF), einen Web-Proxy, ein SMTP-Relay, o. ä. In dieser Zone und an diesen Komponenten terminieren die öffentlichen IP-Adressen, d.h. in allen nachgelagerten Strukturen werden nur interne IP-Adressen vergeben. Alle eingehende und ausgehende Kommunikation ist auf **notwendige Kommunikationsbeziehungen** zu beschränken. Zudem ist in der Webzone keine Anwendungslogik zulässig, d.h. es dürfen dort keine Application Server o. ä. betrieben werden. Dieser **zugangstechnische Übergang vom Internet zu dem Endpunkt eines Cloud-Service ist in Detailstandard #48** genauer geregelt.

Standardisierung

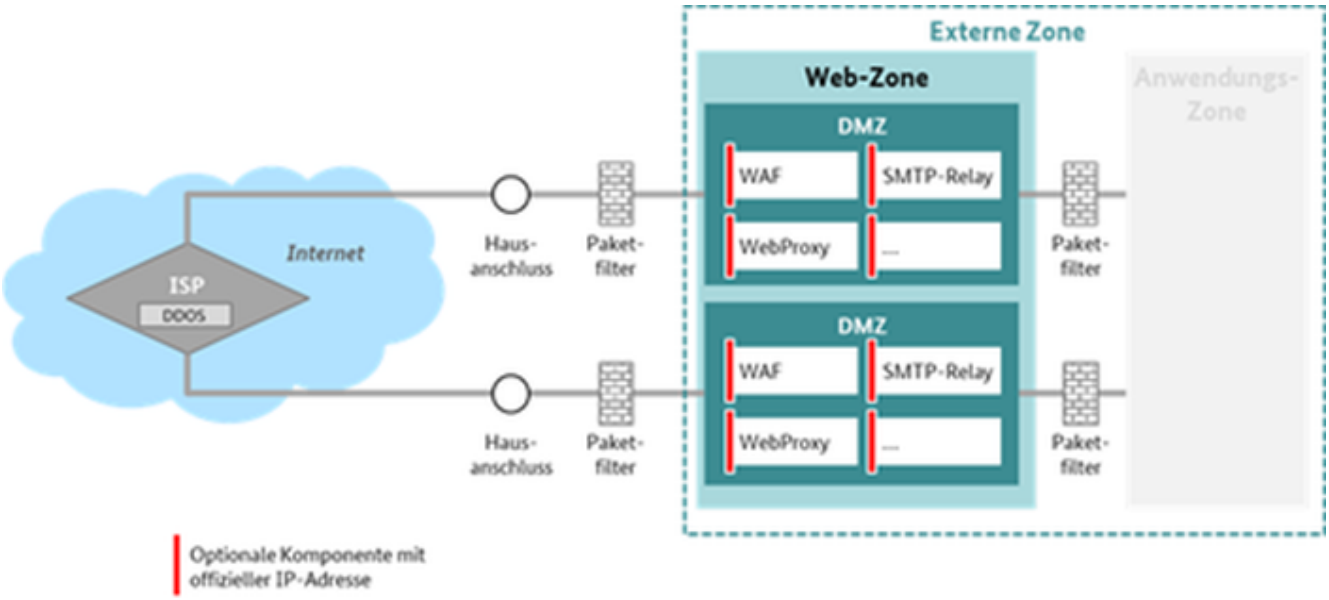

Abbildung 1: P-A-P-Struktur

ID	Rolle	Modal-verb	Detailanforderung
DS_02_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	Die Absicherung **des Internetzugangs und die Absicherung der Verwaltungsnetz MUSS getrennt** sein. Von innen kommender Traffic aus den Verwaltungsnetzen (Kommunale Netze, Landesnetze, NdB-VN, usw.) wird analog der Absicherung ggü. dem (Public) Internet mit P-A-P Struktur über bewusst andere Sicherheitssysteme (eigene P-A-P Systeme) behandelt. Dies, um Angriffe von Seiten der Firewallsysteme dediziert zu trennen. Weitere Details zur Zonierung eines Cloud-Standorts regelt Detailstandard #01 (“Zonenmodell am (DVC) Cloudstandort”)
DS_02_A002	a) **DVC-Plattformbetreiber** b) **DVC-Softwarebetreiber**	SOLL	Sämtliche Netzzugänge SOLLTEN **Bestandteil eines Informationsverbundes** sein, für den der IT-Grundschutz umgesetzt wurde.

Fortsetzung auf nächster Seite

Fortsetzung von vorheriger Seite

ID	Rolle	Modal-verb	Detailanforderung
DS_02_A003	a) **DVC-Plattformbetreiber** b) **DVC-Softwarebetreiber**	MUSS	Bei der **Anbindung des Internets** MUSS eine **P-A-P-Struktur** genutzt werden. Das Application Level Gateway (Webzone in Abbildung 1) enthält Komponenten wie beispielsweise eine Web Application Firewall (WAF), einen Web-Proxy, ein SMTP-Relay, o. ä. In dieser Zone und an diesen Komponenten terminieren die öffentlichen IP-Adressen, d.h. in allen nachgelagerten Strukturen werden nur interne IP-Adressen vergeben. Zudem ist in der Webzone keine Anwendungslogik zulässig, d.h. es dürfen dort keine Application Server o. ä. betrieben werden.
DS_02_A004	a) **DVC-Plattformbetreiber** b) **DVC-Softwarebetreiber**	MUSS	Es MUSS an den Sicherheitssystemen ganzheitlich dem **Schutz des Application Layer** durch geeignete Techniken begegnet werden. Der Einsatz einen Web Application Firewall Systeme zum Schutz webbasierter Systemzugriffe (inkl. Entschlüsselung und Whitelisting der erlaubten Webaufrufe des Content nicht nur der URL) setzt jedoch voraus, dass klassische Intrusion Prevention Funktionen im Bereich der P-A-P Anordnung bspw. für andere Applikationen als webbasierte ebenso umgesetzt sind.
DS_02_A005	a) **DVC-Plattformbetreiber** b) **DVC-Softwarebetreiber**	MUSS	Sämtliche Datenströme MÜSSEN durch die Firewalls der P-A-P-Struktur auf die **notwendigen Protokolle und Kommunikationsbeziehungen** eingeschränkt und dokumentiert werden.
DS_02_A006	a) **DVC-Plattformbetreiber** b) **DVC-Softwarebetreiber**	KANN	Die Webzone ("A" der P-A-P-Struktur) KANN weiter entsprechend **unterschiedlichen Schutzbedarfen segmentiert** werden.
DS_02_A007	a) **DVC-Plattformbetreiber** b) **DVC-Softwarebetreiber**	MUSS	Der Cloud-Standort MUSS eine **redundante Netzanbindung** mit getrennten Leitungswegen sicherstellen.
DS_02_A008	a) **DVC-Plattformbetreiber** b) **DVC-Softwarebetreiber**	MUSS	**IPv4** bei der "Netzanbindung beim Internetzugang" MUSS unterstützt werden.
DS_02_A009	a) **DVC-Plattformbetreiber** b) **DVC-Softwarebetreiber**	SOLL	**IPv6** bei der "Netzanbindung beim Internetzugang" SOLLTE bereits aktuell unterstützt werden.
DS_02_A010	a) **DVC-Plattformbetreiber** b) **DVC-Softwarebetreiber**	MUSS	Der Ausbau auf **IPv6** bei der "Netzanbindung beim Internetzugang" MUSS angestrebt werden
DS_02_A011	a) **DVC-Plattformbetreiber** b) **DVC-Softwarebetreiber**	SOLL	Der Cloud-Standort SOLLTE zwei **Internet Service Provider (ISP)** nutzen.

Fortsetzung auf nächster Seite

Fortsetzung von vorheriger Seite

ID	Rolle	Modal-verb	Detailanforderung
DS_02_A012	a) **DVC-Plattformbetreiber** b) **DVC-Softwarebetreiber**	SOLL	Der Cloud-Standort SOLLTE eine **knoten- und kantendisjunkte Netzanbindung** sicherstellen.
DS_02_A013	a) **DVC-Plattformbetreiber** b) **DVC-Softwarebetreiber**	MUSS	Der Cloud-Standort muss eine **kontinuierliche Kapazitätsplanung für die Netzanbindung** vornehmen.
DS_02_A014	a) **DVC-Plattformbetreiber** b) **DVC-Softwarebetreiber**	SOLL	Der Cloud-Standort SOLLTE beim Internetzugang einen vorgeschalteten Dienst zur **Angriffserkennung und -Abwehr** nutzen. Gemeint ist damit konkret Anti-DDOS bereits beim ISP aufgrund der Bandbreite und Möglichkeiten.
DS_02_A015	a) **DVC-Plattformbetreiber** b) **DVC-Softwarebetreiber**	MUSS	Ein **Security Information and Event Management** (SIEM) MUSS eingesetzt werden
DS_02_A016	a) **DVC-Plattformbetreiber** b) **DVC-Softwarebetreiber**	MUSS	Die **assoziierten Sicherheitssysteme (vergl. DS_02_A014 und DS_02_A015) müssen ausfallsicher (redundant)** ausgelegt sein, damit nicht der Ausfall eines einzigen Systems bereits die Verfügbarkeit beeinträchtigt bei den neuralgischen Infrastrukturpunkten.
DS_02_A017	a) **DVC-Plattformbetreiber** b) **DVC-Softwarebetreiber**	MUSS	Eine **revisisionssichere Protokollierung** MUSS an den Elementen der P-A-P-Struktur und allen assoziierten Sicherheitssystemen (vergl. DS_02_A014 und DS_02_A015) ermöglicht werden entsprechend der jeweiligen Implementierung der teilnehmenden Häuser auf Basis der geltenden rechtlichen Vorgaben.

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 Eine Bundesbehörde
DOS	Denial-Of-Service Ein Angriffsmodell, um angebotene Services lahmzulegen
DDOS	Distributed Denial-Of-Service Ein Angriffsmodell, um angebotene Services von verteilten Angriffspunkten lahmzulegen
DMZ	De-Militarisierte Zone
IDS	Intrusion Detection System Ein System zur aktiven Angriffserkennung
IPS	Intrusion Prevention System Ein System zur aktiven ANgriffsabwehr
ISP	Internet Service Provider Ein Anbieter für Internet-Anbindung
IT Grundschutz	IT Grundschutz Ein vom BSI spezifiziertes Modell, um IT Grundschutz zu gewährleisten auf Basis eines konkreten Vorgabenkatalogds
P-A-P Struktur	Paketfilter - Application Level Gateway - Paketfilter Ein vom BSI genutztes Modell, um Zonenübergänge geeignet abzusichern
SIEM	Security Incident and Event Management Ein technisches und logisches System, um Sicherheitsvorfälle aus eingehenden Daten zu erkennen und zu behandeln