DEUTSCHE VERWALTUNGSCLOUD
EIN PRODUKT DES IT-PLANUNGSRATS

# Detailstandard 17: Schwachstellenscan von Softwarelösungen

Version 1.0 (8.5.2025)

## Inhaltsverzeichnis



## Zusammenfassung


Dieses Dokument beschreibt im Kapitel Anforderungen die zu erfüllenden Anforderungen in diesem Standardisierungsbereich. Im Kapitel Standardisierung werden vorgegebene Architekturen und Realisierungen beschrieben. Diese stellen eine Konkretisierung der beschriebenen Anforderungen dar. Sind im Kapitel Standardisierung keine Vorgaben enthalten, werden keine Einschränkungen zur Erfüllung der Anforderungen definiert.

Aus den BSI Grundschutz Bausteinen OPS.1.1.1.A10 Führen eines Schwachstelleninventars und SYS.1.6.A6 Verwendung sicherer Images ergibt sich, dass Softwarelieferanten und Softwarebetreiber Schwachstellenscans durchführen müssen bzw. sollen. Die Ergebnisse müssen zentral dokumentiert werden. Dieser Detailstandard beschreibt ein am IT-Grundschutz ausgerichtetes, einheitliches Modell zum Umgang mit veröffentlichten Schwachstellen in allen Cloud Standorten.


## Anforderung

Gemäß IT-Grundschutz des BSI ist für betriebene Anwendungen ein Schwachstelleninventar zu führen, welches durch Schwachstellenscans erstellt werden kann.

## Standardisierung

Aus den Vorgaben ergeben sich folgende Detailanforderungen:

| ID | Rolle | Modalverb | Detailanforderung |
|---|---|---|---|
| DS_17_A001 | Softwarelieferant | SOLL | seine gelieferte Software regelmäßig auf Schwachstellen prüfen und die Ergebnisse dokumentieren. |
| DS_17_A002 | Softwarelieferant | SOLL | die Schwachstellenscans in seine Continuous Integration Pipeline einbauen |
| DS_17_A003 | Softwarelieferant | MUSS | bei gefundenen und nicht bereits abgestimmten Schwachstellen eine Abstimmung mit ihm bekannten Softwarebetreibern initiieren mit Fokus auf einem CVSS von 7.0 oder höher vor dem Hintergrund von via BSI als “schwerwiegend” eingestuften Scorewerten und damit etwaiger Auslösung von Security Incidents |
| DS_17_A004 | Softwarebetreiber | MUSS | auf die angelieferte Software vor Inbetriebnahme einen Schwachstellenscan durchführen |
| DS_17_A005 | Softwarebetreiber | SOLL | das Ergebnis des Schwachstellenscans mit dem Ergebnis des Softwarelieferanten abgleichen und abstimmen |
| DS_17_A006 | Softwarebetreiber | MUSS | die Behandlung der Schwachstellen initiieren, nachhalten und sicherstellen |
| DS_17_A007 | Softwarebetreiber | SOLL | die Schwachstellenscans in seine Continuous Deployment Pipelines integrieren |

*Fortsetzung auf nächster Seite*

*Fortsetzung von vorheriger Seite*

| ID | Rolle | Modal-verb | Detailanforderung |
|---|---|---|---|
| DS_17_A008 | Software-betreiber | MUSS | die aktuell eingesetzten Software-Images kontinuierlich auf Schwachstellen prüfen |
| DS_17_A009 | Software-betreiber | MUSS | einen Prozess definieren, der den Umgang mit Schwachstellen festlegt |
| DS_17_A010 | Software-betreiber | MUSS | dem Softwarelieferant - sowie den nachgelagerten Plattformbetreibern jeweils auf Anfrage - den definierten Prozess mitteilen |
| DS_17_A011 | Software-betreiber | MUSS | bei gefundenen nicht abgestimmten Schwachstellen eine Abstimmung mit dem Softwarelieferanten und den nachgelagerten Plattformbetreibern initiieren. Für die Plattformbetreiber ist dies ausschließlich dann relevant, sofern hier bei einer Schwachstelle ein CVSS von 7.0 oder höher vorliegt vor dem Hintergrund zu etwaigen Überlegungen zu Security Incidents. |

## Referenzdokumente

| Kapitel | Seite | Dokument | Version | Link |
|---|---|---|---|---|
| OPS.1.1.1.A10 | 7 | | 2023 | OPS.1.1.1.A10 |
| SYS.1.6.A6 | 6 | | 2023 | SYS.1.6.A6 |
| CVSS Score von 7.0 oder höher | | Leitlinie des BSI zum Coordinated Vulnerability Disclosure (CVD)-Prozess | 2022 | CVD-Leitlinie des BSI |

## Abkürzungsverzeichnis

| Abkürzung | Bezeichnung |
|---|---|
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| OPS | Operations: Betrieb |
| SYS | IT-Systeme |