SRC security consulting

VS-Anforderungsprofile für Infrastrukturkomponenten

Omnisecure Juni 2022

Motivation

- **Welche Anforderungen hat das BSI für Infrastrukturkomponenten formuliert?**
- **Was hat das BSI zu bieten? In welchem Dokument finde ich welche Informationen? -> Produktkatalog, VS-Anforderungsprofile**
- **Kap.4 in den VS-Anforderungsprofilen: Definition der Sicherheitsanforderungen**
- **VS-Verarbeitung im Unternehmen umsetzen – was wird gebraucht?**

© SRC Security Research & Consulting GmbH

Einführung und Übersicht

- **Sicherheitsanforderungen an Infrastrukturkomponenten / IT-Sicherheitsfunktionen nach VSA**
- **Produktklassen gemäß VS-Produktkatalog des BSI**
- **Produkttypen, für die ein VS-Anforderungsprofil vorliegt**
- **Beispiele**

© SRC Security Research & Consulting GmbH

IT-Sicherheitsfunktionen nach VSA

§ 52 IT-Sicherheitsfunktionen

(1) IT-Sicherheitsfunktionen innerhalb von VS-IT, die eine Zulassung des Produktes durch das Bundesamt für Sicherheit in der Informationstechnik nach § 51 Absatz 1 erfordern, sind Funktionen:

1. zur Zugangs- und Zugriffskontrolle,
2. zur Identifikation und Authentisierung,
3. zur kryptographischen Unterstützung,
4. für das Sicherheitsmanagement,
5. zur Informationsflusskontrolle,
6. zum internen Schutz der Benutzerdaten,
7. zum Selbstschutz der Sicherheitsfunktionen und ihrer Daten,
8. zur Netzwerktrennung,
9. zum Schutz der Unversehrtheit,
10. zur Verfügbarkeitsüberwachung oder
11. zur Sicherheitsprotokollierung und Nachweisführung.

Einzelheiten dazu und zum Zulassungskonzept werden in den Technischen Leitlinien des Bundesamtes für Sicherheit in der Informationstechnik geregelt.

(2) Das Bundesamt für Sicherheit in der Informationstechnik gibt einen auf diesen IT-Sicherheitsfunktionen und den sich hieraus ableitenden Produktklassen und -typen basierenden Katalog sowie eine aktuelle Liste zugelassener IT-Sicherheitsprodukte heraus.

© SRC Security Research & Consulting GmbH

Produktklassen gemäß VS-Produktkatalog des BSI

„Katalog von Produktklassen und –Typen gemäß VSA“, Version 1.2, 13.12.2021

- **Netzwerkkopplung**
- **VS verarbeitende Systeme**
- **Indentitätsmanagement und Zugriffskontrolle**
- **Überwachung und Protokollierung**
- **Vertrauenswürdige Separierung**
- **Vertrauenswürdiges IT-Zubehör**
- **Sicherheitsmanagement**
- **Schlüsselmanagement**
- **Kryptomodule**
- **Speicherverschlüsselung**
- **Datenlöschung**
- **Übertragungsverschlüsselung Endgeräte**
- **Übertragungsverschlüsselung Infrastruktur**

© SRC Security Research & Consulting GmbH

Produkttypen, für die ein VS-Anforderungsprofil vorliegt

PRODUKTKLASSE	PRODUKTTYP	VS-ANFORDERUNGSPROFIL
NETZWERKKOPPLUNG	Firewall	BSI-VS-AP-0018-2019_Firewall (VS-NfD
	Datendiode (DDI)	In Erstellung
	VS-Guard (VSG)	BSI-VS-AP-0017-2019_VS-Guard (GEHEIM)
VS VERARBEITENDE SYSTEME	VS-Arbeitsplatz (VAP)	BSI-VS-AP-0007-2020_Sicherer_VS-Arbeitsplatz (VS-NfD)
	VS-Registratursysteme	In Erstellung
	Langzeitarchivierung	Derzeit kein VS-AP
	Digitales Labelling (DL)	BSI-VS-AP-0016-2018_Digitales_Labelling (GEHEIM) BSI-VS-AP-0023-2020_Digitales_Labeling (VS-NfD)
IDENTITÄTSMANAGEMENT UND ZUGRIFFSKONTROLLE	Verzeichnisdienst	Derzeit kein VS-AP
ÜBERWACHUNG UND PROTOKOLLIERUNG	Schadsoftwareerkennung	Derzeit kein VS-AP
	Sicherheitsprotokollierung	Derzeit kein VS-AP
VERTRAUENSWÜRDIGE SEPARIERUNG	Hypervisor	BSI-VS-AP-0019_Hypervisor (VS-NfD) DE/EN *Supporting Document*
	Separation Kernel (SK)	BSI-VS-AP-0015-2019_Separation Kernel (GEHEIM)
VERTRAUENSWÜRDIGES IT-ZUBEHÖR	Sichere Netzwerkkarte (SNK)	BSI-VS-AP-0004-2016_Sichere_Netzwerk_Karte (GEHEIM)
SICHERHEITSMANAGEMENT	Mobile Device Management	Derzeit kein VS-AP
	Netzwerkmagement	Derzeit kein VS-AP
SCHLÜSSELMANAGEMENT	Schlüsselspeicher- und Verteilkomponente	Derzeit kein VS-AP
	Key-Management-Software	Derzeit kein VS-AP
KRYPTOMODULE	HSM / Kryptobeschleuniger	BSI-VS-AP-0002-2018_Hardware_Sicherheits_Modul (VS-NfD) BSI-VS-AP-0013-2017_Hardware_Sicherheits_Module (GEHEIM)
	Sicherheitsanker (HW-SiA)	BSI-VS-AP-0022-2021-Hardware-Sicherheitsanker (VS-NfD) *Supporting Document*
	Verschlüsselungsgeräte für Funksysteme	Derzeit kein VS-AP
	Verschlüsselungsgeräte für Satellitensysteme	Derzeit kein VS-AP
	Verschlüsselungsgeräte für analoge Leitungen	Derzeit kein VS-AP
SPEICHERVERSCHLÜSSELUNG	Dateiverschlüsselung	Derzeit kein VS-AP
	Festplattenverschlüsselung (FPV)	BSI-VS-AP-0008-2018 Festplattenverschlüsselung (VS-NfD)
	Sicherer mobiler Datenträger (SMD)	BSI-VS-AP-0006-2018_Sicherer_Mobiler_Datenträger (VS-NfD)
DATENLÖSCHUNG	Degausser	Derzeit kein VS-AP
	Datenlöschsoftware	Derzeit kein VS-AP
ÜBERTRAGUNGSVERSCHLÜSSELUNG ENDGERÄTE	Faxverschlüsselung	Derzeit kein VS-AP
	Telefonverschlüsselung	Derzeit kein VS-AP
	Funkgeräte	Derzeit kein VS-AP
	E-Mail- und Dateiverschlüsselung (EuDV)	BSI-VS-AP-0014-2018_Sichere_Uebertragung_von_E-Mails_und_Dateien (VS-NfD) In Überarbeitung: BSI-VS-AP-0014-2022_E-Mail_und_Dateiaustausch-Verschluesselung (VS-NfD)
	VPN-Client (VPNC)	BSI-VS-AP-0005-2017_VPN-Client (VS-NfD)
	Sichere Mobile Lösung (SML)	BSI-VS-AP-0003-2017_Sichere_Mobile_Lösung (VS-NfD)
ÜBERTRAGUNGSVERSCHLÜSSELUNG INFRASTRUKTUR	Verschlüsselung Layer 1	Derzeit kein VS-AP
	Verschlüsselung Layer 2 (L2V)	BSI-VS-AP-0010-2021-Layer2Verschluessler (VS-NfD)
	VPN-Gateway (VPNG)	BSI-VS-AP-0001-2021-VPN-Gateway (VS-NfD)
	E-Mailverschlüsselung	Derzeit kein VS-AP

© SRC Security Research & Consulting GmbH

VS-Anforderungsprofile

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Zulassung/VS-Anforderungsprofile/vs-anforderungsprofile_node.html

© SRC Security Research & Consulting GmbH

Liste zugelassener Produkte

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Zulassung/Liste-zugelassener-Produkte/liste-zugelassener-produkte_node.html

© SRC Security Research & Consulting GmbH

Beispiele zugelassener Produkte nach einem VS-Anforderungsprofil

- **VPN-Client**
  - genua GmbH, Produkt „genuconnect“, BSI-VSA-10641
  - NCP engineering GmbH, Produkt „ NCP VS GovNet Connector“, BSI-VSA-10599
  - Rohde&Schwarz Cypersecurity GmbH, Produkt „ R&S®Trusted VPN Client“, BSI-VSA-10597
  - ECOS Technology GmbH, Produkt „ ECOS Secure Boot Stick”, BSI-VSA-10622
- **Sicherer Mobiler Datenträger**
  - DIGITTRADE GmbH, Produkt „Kobra Drive VS und Kobra Stick VS“, BSI-VSA-10338

© SRC Security Research & Consulting GmbH

VS-Anforderungsprofil - Zweck

„Bei diesem Dokument handelt es sich um ein VS-Anforderungsprofil des BSI an einen Produkttyp. Zulassungsrelevante Produkttypen sind im Dokument „VS-Produktkatalog des BSI“ [2] aufgeführt. Produkte dieses Typs übernehmen IT-Sicherheitsfunktionen innerhalb von Informationstechnik zur Handhabung von Verschlusssachen (VS-IT) im Sinne der VSA [3], § 52.

Dieses Dokument vermittelt zulassungsrelevante Anforderungen an Produkte, welche zum in dem VS-Anforderungsprofil genannten Produkttyp gehören. Die Bewertung für die prinzipielle Eignung solcher Produkte für den vom Bedarfsträger gewünschten Einsatzzweck wird sich u.a. darauf abstützen, inwiefern die Anforderungen von einem Produkt erfüllt werden.

Auch Hersteller eines Produktes können das VS-Anforderungsprofil nutzen, um einen ersten Eindruck von den Anforderungen an einen Produkttyp zu gewinnen. Abweichungen bei der Umsetzung der hier definierten Anforderungen in einem Produkt sind, sofern mit dem BSI abgestimmt, in begründeten Fällen möglich. Eine Prüfung der Erfüllung dieses VS-Anforderungsprofils ersetzt nicht den Prozess der Zulassung eines Produktes durch das BSI. Diese erfolgt gemäß dem Nachweiskatalog [1]. Mit der Technischen Leitlinie des BSI [4] werden den im Zulassungsprozess eingebundenen Akteuren Hinweise zur Unterstützung einer VSA- und Zulassungsschema-konformen Handlungsweise gegeben. In diesem Dokument wird ferner auf Anforderungen der EU/NATO hingewiesen. Auch hier ersetzt eine Prüfung der Erfüllung dieser Anforderungen nicht die Zulassung durch die jeweils zuständigen Stellen.“

© SRC Security Research & Consulting GmbH

VS-Anforderungsprofil - Ziel

- **Ein VS-Anforderungsprofil (kurz: VS-AP) soll Herstellern und Betreibern auf verständliche Weise darstellen, welche Sicherheitsanforderungen ein Produkttyp erfüllen muss, damit eine Zulassung für ein konkretes Produkt zum Schutz eingestufter Daten in Betracht gezogen werden kann.**
- **Die tatsächliche Zulassung des Produktes erfolgt gemäß dem Nachweiskatalog des BSI „Nachweise für eine Evaluierung für eine Zulassung bis VS-NfD bzw. VS-VERTRAULICH/GEHEIM“.**
- **Ein VS-AP ersetzt nicht das für eine Zulassung des Produktes notwendige Security Target sowie die weitere Dokumentation des Herstellers.**

© SRC Security Research & Consulting GmbH

VS-Anforderungsprofil – Inhalt

- **Beschreibung des Produkttyps**
- **Definition des Sicherheitsproblems**
- **Sicherheitsziele**
- **Sicherheitsanforderungen**
- **Hinweise zur Umsetzung der Sicherheitsanforderungen**
- **Hinweise zum sicheren Betrieb des Produktes**

© SRC Security Research & Consulting GmbH

Beispiel: Hardware-Sicherheitsanker (HW-SiA)

Beschreibung des Produkttyps	Ein Hardware-Sicherheitsanker (HW-SiA) ist ein Produkttyp, der sich durch die beiden folgenden grundlegenden IT-Sicherheitsfunktionen auszeichnet: • Ein HW-SiA ist in der Lage, besonders schützenswerte Daten sicher zu speichern, wobei der Schutz insbesondere hardwaretechnische Maßnahmen umfassen muss. Besonders schützenswerte Daten zeichnen sich dadurch aus, dass sie nur im Klartext abgelegt und zu ihrem Schutz nicht verschlüsselt werden können. Sie fungieren oft als „Urgeheimnisse“ in dem Sinne, dass sie am Anfang einer Vertrauenskette stehen und daher unverschlüsselt verfügbar sein müssen. Zu solchen Urgeheimnissen zählen beispielsweise kryptographische Schlüssel wie Root-Zertifikate, Key-Encryption-Keys und Master-Keys. Aber auch Passwörter, PINs und andere Daten, die nur im Klartext vorliegen, können besonders schützenswert sein. • Bevor es einem Nutzer erlaubt ist, mit besonders schützenswerten Daten Operationen auszuführen, muss dieser gegenüber dem HW-SiA erfolgreich authentisiert sein. Ein HW-SiA besteht immer aus dedizierter Hardware einschließlich notwendiger Soft- und Firmware. In diesem VS-Anforderungsprofil werden keine Einschränkungen für mögliche Bauformen eines HW-SiA gemacht.
IT-Sicherheitsfunktionen (gemäß Produktkatalog des BSI)	zur kryptographischen Unterstützung zur Identifikation und Authentisierung zur Zugangs- und Zugriffskontrolle zum Selbstschutz der Sicherheitsfunktionen und ihrer Daten
Sicherheitsanforderungen	Anf.HardwareSecurity Anf.DataProtection Anf.AccessControl Anf.Authentication Anf.AuthenticationMechanism Anf.Crypto Anf.Random Anf.Certificates Anf.KeyManagement Anf.Residual Anf.SecurityManagement Anf.Selftest

© SRC Security Research & Consulting GmbH

Beispiel: E-Mail- und Dateiaustausch-Verschlüsselung (EuDV)

Beschreibung des Produkttyps	Die E-Mail- und Dateiaustausch-Verschlüsselung (EuDV) ist ein Produkttyp, der die Vertraulichkeit, Integrität und Authentizität beim Austausch von sensiblen Daten zwischen Nutzern sicherstellt. Die E-Mails bzw. die Dateien sollen von einem Nutzer (Absender) zu einem anderen Nutzer (Empfänger) so übertragen, versendet bzw. transportiert werden, dass folgende Ziele erreicht werden können, sofern der Nutzer die von der EuDV angebotenen Sicherheitsfunktionen entsprechend nutzt: Vertraulichkeit der Daten, Integrität der Daten, Authentizität der Daten bzw. des Absenders der Daten.
IT-Sicherheitsfunktionen (gemäß Produktkatalog des BSI)	zur kryptographischen Unterstützung zur Identifikation und Authentisierung zur Zugangs- und Zugriffskontrolle
Sicherheitsanforderungen	Anf.Encryption Anf.Decryption Anf.IntegrityAndAuthenticity Anf.Access Anf.Authentication Anf.KeyManagement Anf.Random Anf.Certificates Anf.Administration Anf.Logging Anf.Selftest Anf.Update

© SRC Security Research & Consulting GmbH

Beispiel: E-Mail- und Dateiaustausch-Verschlüsselung (EuDV)

- **Aktuell befindet sich das VS-AP in Überarbeitung (früher: Sichere Übertragung von E-Mails und Dateien, jetzt: E-Mail- und Dateiaustausch-Verschlüsselung)**
- **Veröffentlichung erfolgt demnächst**
- **Berücksichtigung eines Hardware-Sicherheitsankers**
- **Aufteilung Anforderungen TOE/Einsatzumgebung (HW-SiA, Schlüsselmanagement, Logging)**

© SRC Security Research & Consulting GmbH

Weitere Beispiele im Überblick

PRODUKTTYP	SICHERHEITSANFORDERUNGEN
Firewall	Anf.Paketfilter, Anf.ALG, Anf.Adresse, Anf.Audit_Trail, Anf.Authentisierung, Anf.Kommunikation, Anf.Management, **Anf.Logging**, **Anf.Update**, **Anf.Selbsttest**, **Anf.Krypto**
VS-Guard	…
Digitales Labelling	…
Festplattenverschlüsselung & Sicherer VS-Arbeitsplatz	Anf.Authentisierung, Anf.Speicherung, Anf.Verschlüsselung, **Anf.Zufallszahlengenerator**, **Anf.Zertifikate**, Anf.Schlüsselmanagement, Anf.Administration, **Anf.Selbsttest**, **Anf.Update**, **Anf.Logging**, Anf.Management Sicherer VS-Arbeitsplatz zusätzlich: Anf.Schnittstellenkontrolle, Anf.Firewall_und_Schutz_vor_Schadsoftware, Anf.Plattform
VPN-Client	Anf.K.Gegenseitige_Authentisierung, Anf.K.Übertragungsverschlüsselung, **Anf.K.Krypto**, **Anf.K.Zufallszahlengenerator**, **Anf.K.Zertifikate**, Anf.K.Integritätsschutz, Anf.K.Schlüsselmanagement, **Anf.K.Hardware_Sicherheit**, Anf.K.Admin_Authentisierung Anf.Informationsflusskontrolle, Anf.Management, **Anf.Update**, **Anf.Logging**, Anf.Authentisierung, Anf.Speicherung
VPN-Gateway	Anf.DataProtection, Anf.Integrity, Anf.MutualAuthentication, Anf.SessionKeys, **Anf.Certificates**, **Anf.Crypto**, **Anf.Random**, Anf.KeyManagement, **Anf.HardwareSecurity**, Anf.AdminAuthentication, Anf.InformationsflowControl, Anf.Management, **Anf.Logging**, **Anf.Selftest**, **Anf.Update**, *Anf.SecurityArchitecture*
Sicherer Mobiler Datenträger	…
Sichere Mobile Lösung	Sicherheitsanforderungen an die Endgeräte, an das mobile Betriebssystem, an die Software/Apps, an den Übertragungskanal, an den Zugang zur Infrastruktur der SML, an den Synchronisations- und Administrationsserver und an das Zertifikatsmanagement
Layer-2-Verschlüsseler	Anf.DataProtection, Anf.KeyManagement, Anf.Authentication, **Anf.Crypto**, **Anf.Random**, **Anf.Certificates**, Anf.InformationflowControl, Anf.AccessControl, Anf.AdminAuthentication, Anf.SecurityManagement, **Anf.Logging**, **Anf.Selftest**, **Anf.Update**

© SRC Security Research & Consulting GmbH

Fazit

- **BSI stellt mit den VS-APs „Standards“ für die Zulassung bereit**
- **VS-APs enthalten Sicherheitsanforderungen zu einem Produkttyp**
- **Kernziel: Schutz der sensiblen Daten**
- **Für diverse Infrastrukturkomponenten liegen bereits VS-APs vor (über BSI-Webseite verfügbar)**
- **Umsetzung in der Praxis …**

© SRC Security Research & Consulting GmbH

Kontakt

Dr. Bertolt Krüger
Security Research & Consulting GmbH
Emil-Nolde-Str. 7
53113 Bonn

Tel. +49-(0)228-2806-122
Fax: +49-(0)228-2806-199
E-mail: bertolt.krueger@src-gmbh.de
https://www.src-gmbh.de

© SRC Security Research & Consulting GmbH