Bundesamt
für Sicherheit in der
Informationstechnik

SRC
security consulting

Bewertung des Angriffspotentials in VS-Zulassungsverfahren

Omnisecure 2022

Problemstellung

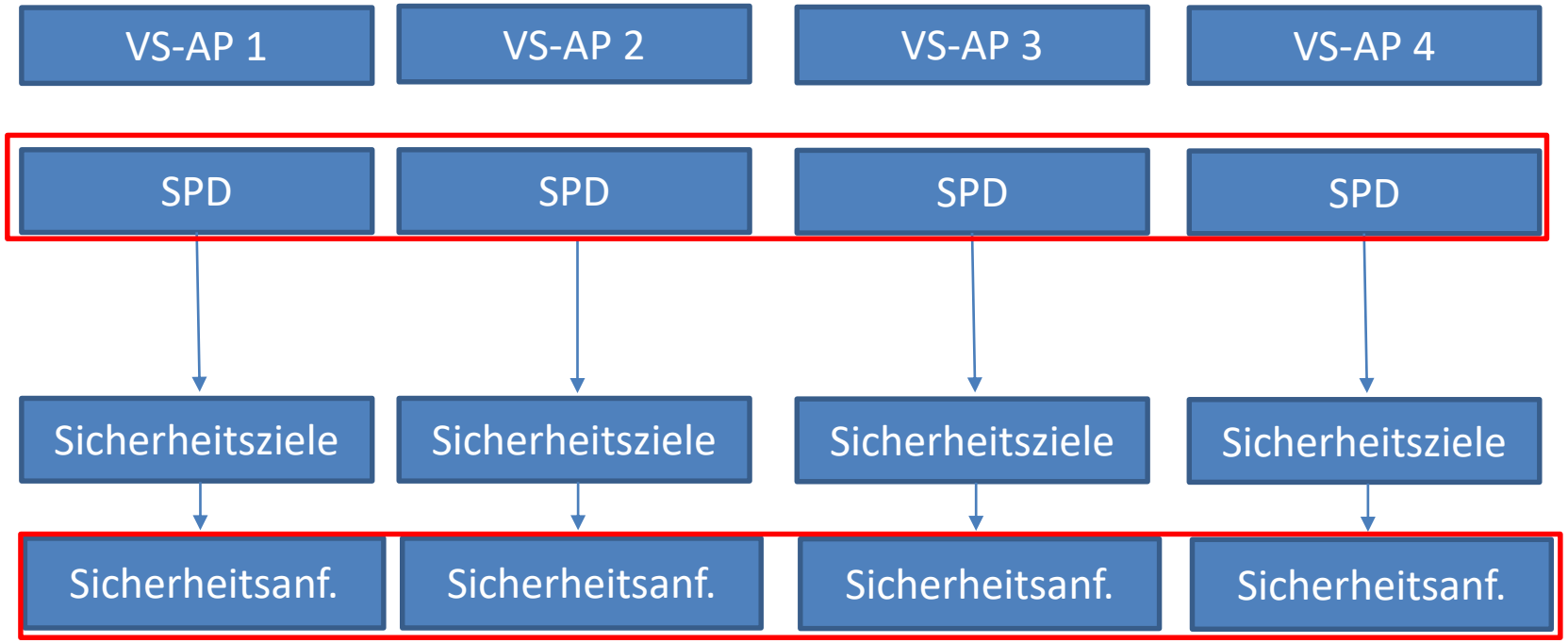
- **Problem 1: Viele berechtigte Fragen zur Angemessenheit der Sicherheitsanforderungen in Zulassungsverfahren**
  - **Beispiele folgen!**
- **Problem 2: Die „Common Criteria“ (CC), die den Zulassungsverfahren für IT-Produkte zugrunde liegt, misst Angriffsstärke nach Fähigkeiten und Ressourcen des Angreifers. Die Definition der VS-Stufen bezieht sich aber eher auf den angerichteten Schaden bei Verlust eines Dokuments.**
  - **Dies aufeinander abzubilden, ist nicht trivial!**
- **Wir müssen Problem 2 adressieren, um Problem 1 angemessen beantworten zu können.**
- **Dazu läuft ein Projekt im BSI, zu dem hiermit ein Zwischenstand gegeben wird.**

1. Beispiel für Problem 1

Angemessenheit der Sicherheitsanforderung auf Basis der Angriffsstärke erscheint manchmal nicht plausibel:

Ein VS-NfD Papierdokument darf mit normaler Briefpost verschickt werden, aber für das IT-Produkt wird eine 2-Faktor-Authentisierung verlangt? Wie passt das zusammen?

2. Beispiel für Problem 1:



Bisher fehlt der horizontale Vergleich zwischen den VS-AP:
Gleiche Sicherheitsanforderung in scheinbar gleicher Situation?
(z.B. mal mit mal ohne Hardware-Sicherheitsanker).

Inhaltsübersicht

1. Sachstand: Wie macht es die CC?
2. Sachstand: Wie sind die heutigen Festlegungen der Angriffsstärke bei der VS-Zulassung?
3. Bedarf: Welche Faktoren sollten künftig (stärker) berücksichtigt werden?
4. Vorgehen: Wie soll die an die CC angelehnte Vorgehensweise modifiziert werden, um Problem 2 zu adressieren?

Bundesamt für Sicherheit in der Informationstechnik

Wie macht es die Common Criteria? (1)

- Um die Prüftiefe eines CC-verfahrens festzulegen, wählt man im allgemeinen eine EAL-Stufe
  - EAL Evaluation Assurance Level, von EAL1 bis EAL7
  - Beispiel EAL4: „**methodically designed, tested, and reviewed** “
- Die EAL-Stufe umfasst viele Prüfaktivitäten, unter anderen die Schwachstellenanalyse, formal bezeichnet als AVA_VAN (Assurance class Vulnerability Assessment – Vulnerability Analysis)
  - EAL4 enthält z.B. die Stufe AVA_VAN.3, damit soll das untersuchte Produkt resistent gegen Angreifer der Stärke „Enhanced Basic“ sein. (Bedeutung: siehe Folgefolien)

Wie macht es die Common Criteria? (2)

- **Die CC definiert folgende Angriffsstärken:**

Vulnerability Component	TOE resistant to attacker with attack potential of:	Residual vulnerabilities only exploitable by attacker with attack potential of:
VAN.5	High	Beyond High
VAN.4	Moderate	High
VAN.3	Enhanced-Basic	Moderate
VAN.2	Basic	Enhanced-Basic
VAN.1	Basic	Enhanced-Basic

- **(diese und folgende Tabellen stammen aus der Common Evaluation Methodology CEM)**

Wie macht es die Common Criteria? (3)

- **Messung der Angriffsstärke: Dazu werden Fähigkeiten und Ressourcen des Angreifers bewertet (genannt „Faktoren“):**

a) Time taken to identify and exploit (***Elapsed Time***);

b) Specialist technical expertise required (***Specialist Expertise***);

c) Knowledge of the TOE design and operation (***Knowledge of the TOE***);

d) ***Window of opportunity***;

e) ***IT hardware/software or other equipment*** required for exploitation.

Bundesamt
für Sicherheit in der
Informationstechnik

Wie macht es die Common Criteria? (3)

- **Messung der Faktoren (diese werden dann addiert):**

Factor	Value
Elapsed Time	
<= one day	0
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19
Expertise	
Layman	0
Proficient	3*(1)
Expert	6
Multiple experts	8
Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of Opportunity	
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	**(2)
Equipment	
Standard	0
Specialised	4(3)
Bespoke	7
Multiple bespoke	9

Wie macht es die Common Criteria? (4)

- **Auswertung:**

Values	Attack potential required to exploit scenario:	TOE resistant to attackers with attack potential of:	Meets assurance components::	Failure of components:
0-9	Basic	No rating	-	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
10-13	Enhanced-Basic	Basic	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
14-19	Moderate	Enhanced-Basic	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5
20-24	High	Moderate	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
=>25	Beyond High	High	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	-

Bundesamt für Sicherheit in der Informationstechnik

Heutige Festlegungen in der VS-Zulassung

- **Für Produkte, die Dokumente der Stufe VS-NfD schützen sollen: Entspricht AVA_VAN.4, d.h. soll resistent gegen Angreifer der Stärke „moderate“ sein**
- **Für Produkte, die Dokumente der Stufe VS-vertraulich oder höher schützen sollen: Entspricht AVA_VAN.5, d.h. soll resistent gegen Angreifer der Stärke „hoch“ sein**
- **Charakteristik: Es wird die Messmethode der CC (siehe vorige Folien) für die Bestimmung der Angriffsstärke verwendet.**

Bundesamt
für Sicherheit in der
Informationstechnik

Künftig stärker zu berücksichtigende Faktoren (1)

Motivation des Angreifers

Dies ist in der bisherigen CC-Bewertung nur indirekt enthalten und damit schwer zu bewerten

Script Kiddie	Organisation
	
Spaß am Probieren	Kriminelle Energie

Künftig stärker zu berücksichtigende Faktoren (2)

Risiko des Angreifers

Es geht nicht nur darum, wie „leicht“ ein Angriff im technischen Sinne ist, sondern welches Risiko ein Angreifer einzugehen bereit ist

Strafgesetzbuch (StGB)

§ 202 Verletzung des Briefgeheimnisses

(1) Wer unbefugt

1. einen verschlossenen Brief oder ein anderes verschlossenes Schriftstück, die nicht zu seiner Kenntnis bestimmt sind, öffnet oder
2. sich vom Inhalt eines solchen Schriftstücks ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,

wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in § 206 mit Strafe bedroht ist.
(2) Ebenso wird bestraft, wer sich unbefugt vom Inhalt eines Schriftstücks, das nicht zu seiner Kenntnis bestimmt und durch ein verschlossenes Behältnis gegen Kenntnisnahme besonders gesichert ist, Kenntnis verschafft, nachdem er dazu das Behältnis geöffnet hat.
(3) Einem Schriftstück im Sinne der Absätze 1 und 2 steht eine Abbildung gleich.

Künftig stärker zu berücksichtigende Faktoren (3)

Zudem sind verschiedene Angriffsvektoren zu unterscheiden: Es ist ein großer Unterschied, ob man anonym Daten abhört, die über das Internet übertragen werden, oder ob man sich in ein Büro schleichen muss, um sich an einem fremden Rechner einzuloggen.

Zu Hause	Bürogebäude
	
Niemand sieht einen	Vorbei an Mitarbeitern …

Bundesamt für Sicherheit in der Informationstechnik

Künftig stärker zu berücksichtigende Faktoren (4)

Aufwand für den Benutzer/Betreiber

Wenn die Einhaltung von Sicherheitsvorschriften zu schwierig ist („Wähle ein zwanzig Zeichen langes Passwort und wechsle es alle drei Monate!“), dann besteht das Risiko, dass die Sicherheitsmechanismen umgangen und dadurch nutzlos werden

Dies wird in klassischer CC (fast) gar nicht berücksichtigt!

Benutzeraufwand	Wert der Schutzmaßnahme

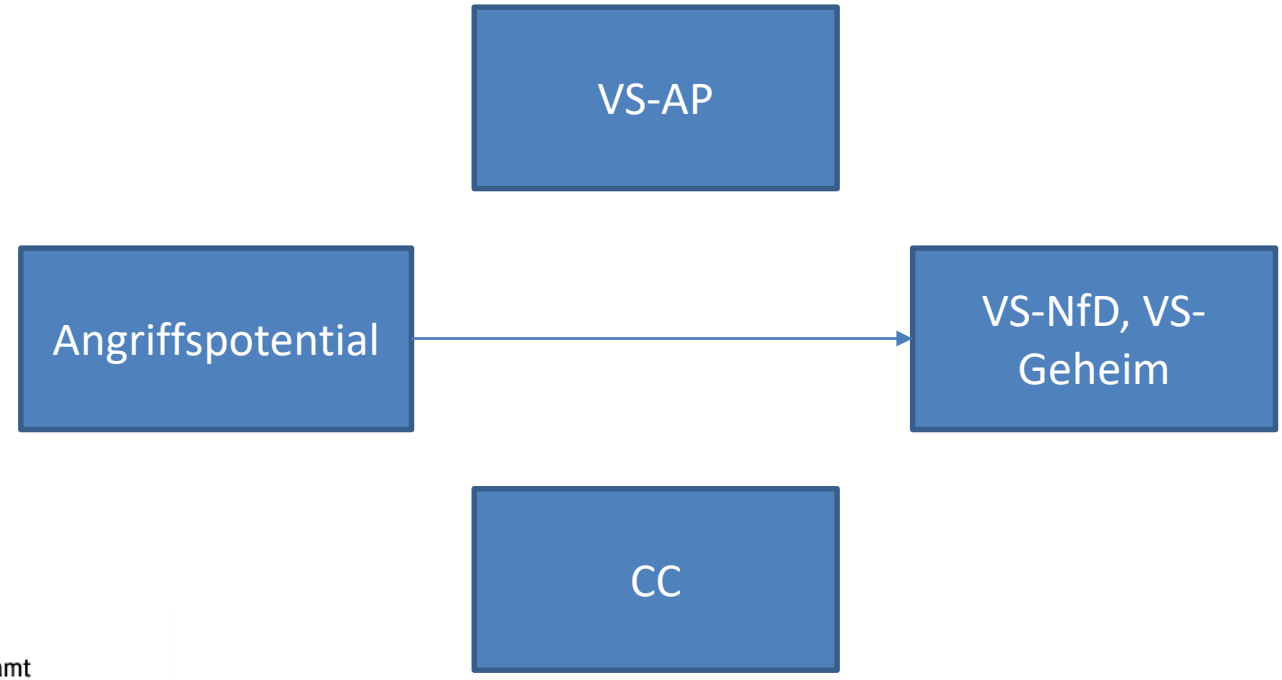
Bundesamt für Sicherheit in der Informationstechnik

Zusatzziel

- **Kann man bestimmte Grundsatzentscheidungen ein Mal treffen, ohne sie für jeden Produkttyp neu diskutieren zu müssen?**
  - **Z.B.: Brauche ich für VS-NfD eine 2-Faktor-Authentisierung?**
  - **Dies geht strenggenommen über den reinen Aspekt „Angriffspotential“ hinaus, das Ziel ist aber dasselbe: Nicht bei jedem Produkt dieselben Diskussionen erneut führen zu müssen.**

Weitere Vorgehensweise

- **Definiton neue Komponenten AVA_VAN.xyz unter Berücksichtigung neuer Faktoren**
- **„Feintuning“ mittels Punktebewertung**



Bundesamt für Sicherheit in der Informationstechnik

Umfrage

- **Abholbar am Stand des BSI**

Kontakt

SRC
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

Bundesamt
für Sicherheit in der
Informationstechnik