Von der Produktzulassung zur Herstellerqualifizierung

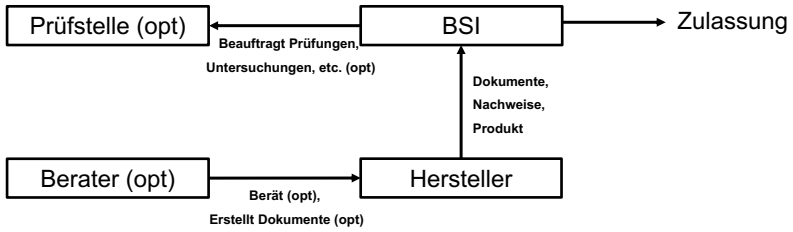
Michael Vogel - atsec information security, V1.0, 03.06.2022

mvogel@atsec.com

1

[Produkt-]Zulassungen

- Zulassungen werden nur aufgrund eines bestehenden Bedarfs erteilt.
- "Die [Produkt-]Zulassung ist eine verbindliche Aussage zum Sicherheitswert eines IT-Sicherheitsproduktes. Nach der Erteilung einer Zulassung für ein IT-Sicherheitsprodukt dürfen Verschlusssachen (VS) gemäß Sicherheitsüberprüfungsgesetz bis zum Zulassungsgrad, für den die Zulassung maximal erteilt wurde, mit diesem IT-Sicherheitsprodukt verarbeitet oder übertragen werden." *



* FAQ des BSI zur Zulassung, https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Zulassung/FAQ-Evaluierung-und-Zulassung/faq-evaluierung-und-zulassung_node.html

2

Umfang und Häufigkeit von Zulassungen

- Umfang der Prüfung für Zulassungsprojekte: gemäß 'Nachweiskatalogen' (Weitergabe nur nach Zustimmung des BSI gestattet.)
- "In etwa vergleichbar mit CC EAL4+"
- Wachsende Zahl an VS-Anforderungsprofilen (ähnlich zu CC Protection Profiles) (z.T. eingestuft)

Häufigkeit:

- Hersteller mit einem Produkt, das für drei Jahre stabil bleibt -> ein Zulassungsverfahren in drei Jahren
- Hersteller mit fünf Produkten und drei neue Produktversionen pro Produkt und Jahr -> Potenziell 15 Zulassungsverfahren pro Jahr =>

➢ **Entlastung aller beteiligten Instanzen durch Herstellerqualifizierung**

3

Einführung Herstellerqualifizierung - I

Problem:

- Effizienz (Dauer, Kosten, Ressourcen) des Zulassungsverfahrens steigern ohne dabei die Qualität der Sicherheitsaussage zu mindern

Idee:

- Wesentliche Aspekte eines Qualifizierten Zulassungsverfahrens
  - Durchführung einer konzeptionellen statt vollständig technischen Prüfung
  - Im Rahmen eines Qualifizierten Zualssungsverfahrens werden ASE, eine informelle Architekturbeschreibung und ein informelles Kryptokonzept geprüft.
  - Herstellererklärung
- Feststellung der Eignung eines Herstellers zur Teilnahme am Qualifizierten Zulassungsverfahren durch "entkoppeltes" Verfahren der Herstellerqualifizierung
  - Prozessbezogene Prüfungen (ALC) sind nicht produktspezifisch
  - Stärkere Automatisierung (Tools) reduziert Fehleranfälligkeit und damit Prüfungsaufwand

4

Einführung Herstellerqualifizierung - II

- Hersteller haben ein Managementsystem, das alle Prozesse des Lebenszyklus von Zulassungsprodukten umfasst (ALC)
  - Planung, Entwicklung, Test, Produktion, Maintenance, Abkündigung
  - Alle Zulassungsnachweise werden innerhalb dieser Prozesse erstellt und gepflegt.
- Auf dieser Basis vertraut das BSI den Herstellern, dass durch Anwendung der durch das BSI geprüften Prozesse zulassungskonforme IT-Sicherheitsprodukte entstehen, ohne dass eine vollumfängliche technische Prüfung erforderlich ist
- Zulassungsverfahren, die im Rahmen des Qualifizierten Verfahrens abgewickelt werden, werden dadurch beschleunigt
- Verfahren der Herstellerqualifizierung prüft initial die Qualität des MS und danach regelmäßig die Einhaltung der Verfahren

5

Anforderungen 'Life-cycle Support' (ALC)

Prüfaspekt	Zulassung	CC EAL4	Herstellerq.
ALC_CMC (Konfigurationsmanagementsystem)	opt.	4	5*
ALC_CMS (Konfigurationsliste)	3	4	5*
ALC_DEL (Auslieferungsprozess)	opt	1	1*
ALC_DVS (Sicherheit der Entwicklungsumgebung)	opt	1	1*
ALC_FLR (Fehlerbehebung)	3*	opt	3*
ALC_LCD (Lebenszyklusbeschreibung)	opt	1	1*
ALC_TAT (Entwicklungswerkzeuge)	opt	1	3*

* Vom BSI angepasste Komponenten, die auf CC-Komponenten basieren.

Die ALC-Anforderungen der Herstellerqualifizierung entsprechen in etwa denen von **CC EAL6** (außer ALC_DVS).

6

Anforderungen 'Konfigurationsliste' (CMS)

- Konfigurations(stand)liste wie bisher (ALC_CMS.3): Der EVG selbst; die Herstellernachweise (Evaluierungsdokumente); die Anteile, die den EVG bilden; die Implementierungsdarstellung
- Zusätzlich zu verwalten:
  - "Security Flaws + Resolution Status": Liste aller bekannten 'sicherheitskritischen Fehler' und deren Status. Ziel ist es, einen Prozess zu haben, um alle sicherheitsrelevanten Fehler systematisch zu erfassen, und sicherzustellen, dass vor der Produktfreigabe alle bekannten sicherheitsrelevanten Fehler behoben wurden.
  - "Entwicklungswerkzeuge und verwandte Informationen (z.B. Toolkonfigurationen)": Verwaltung z.B. von Compilern in GIT.
- ALC_CMS definiert die Liste der "configuration items". => Grundlage für ALC_CMC (Anforderungen an das Konfigurationsmanagementsystem)
- CM-Tools können Konfigurationslisten automatisch erzeugen
- Ticket-Systeme helfen beim Tracking von Sicherheitsproblemen

7

Anforderungen 'Auslieferung' (DEL)

- Dokumentation der Prozesse zur (sicheren) Auslieferung des zuzulassenden IT-Sicherheitsproduktes (bzw. Teile davon wie zum Beispiel Benutzerdokumentation) an den 'Benutzer' (z.B. Endkunde, Systemintegrator) -> konsistent mit Beschreibungen in der Nutzerdokumentation (AGD)
- Die Dokumentation muss beschreiben, wie die Sicherheit des Evaluierungs-gegenstandes während der Auslieferung an den Benutzer gewährleistet wird
- Anwendung und Einhaltung der beschriebenen Prozesse

Quelle: https://www.pexels.com/de-de/foto/boot-im-gewasser-262353/

8

Anforderungen 'Sicherheit der Entwicklungs-umgebung (DVS)'

- Dokumentation der Sicherheit der Entwicklungsumgebung
- Dokumentation muss alle
  - Physischen
  - Prozeduralen
  - Personellen
  - Und anderen

Sicherheitsmechanismen beschreiben, welche notwendig sind, um die Vertraulichkeit (?) und Integrität des TOE-Designs und der Implementierung innerhalb der Entwicklungsumgebung zu gewährleisten.

Quelle: https://www.pexels.com/de-de/foto/graues-betongebaude-unter-grauem-und-weissem-himmel-wahrend-des-tages-64287/

- **Audit/Site Visit (für alle ALC-Aspekte!)**

9

Anforderungen 'Flaw Remediation (FLR)'

- Gilt unverändert, Wechselwirkung mit ALC_CMC/CMS; Audit

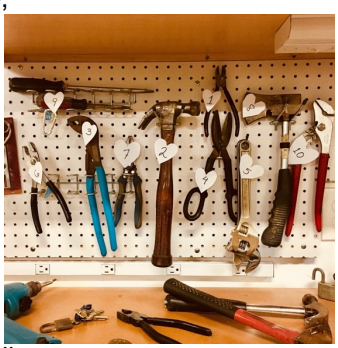
10

Anforderungen 'Life-Cycle Support (LCD)'

- Dokumentation eines Lebenszyklus-Modells zur Entwicklung und Pflege zuzulassender IT-Sicherheitsprodukte ('EVGs'), das die notwendige Kontrolle über die Entwicklungs- und Pflegephasen beinhaltet und einen Überblick über die ALC Aspekte bietet ('Einstieg' in die Herstellerqualifizierung).
- Das dokumentierte Modell muss bei der Entwicklung und Pflege des EVGs verwendet werden.
- => Typischerweise Lebenszyklusmodell, das den Vorgaben des Qualitätsmanagements eines Unternehmens entspricht (Sammlung von Anforderungen; Verabschiedung des Anforderungskatalogs; Implementierung; Verifikation; Meilensteine/ Quality Gates, Abnahmeprozeduren; Freigabe, EOL); Welche Tools werden zur Kontrolle eingesetzt?

Anforderungen 'Tools & … (TAT)'

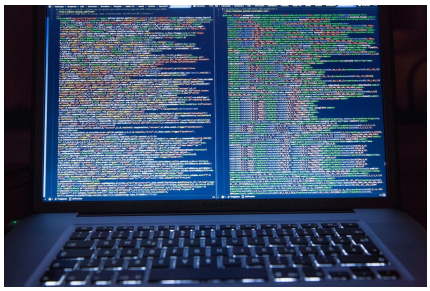
- Dokumentation aller Entwicklungswerkzeuge, die für zuzulassende IT-Sicherheitsprodukte verwendet werden.
- Alle Entwicklungswerkzeuge müssen wohldefiniert sein.
- Beschreibung aller gewählten implementierungsabhängigen Optionen und deren Bedeutung für alle Entwicklungs-Werkzeuge.
- Die Beschreibung jedes Entwicklungs-werkzeuges muss eindeutig die Bedeutung aller Anweisungen, Konventionen und Befehle definieren, die in der Implementierung verwendet werden (z.B. Compiler-Switches)



Quelle: https://www.pexels.com/de-de/foto/handheld-tools-hangen-an-der-workbench-909256//

Anforderungen '… Techniques (TAT)'

- Beschreibung aller Implementierungsstandards, die vom Entwickler des EVGs und allen Drittanbietern, die Teile des EVGs entwickelt haben, angewandt wurden.
- Verwendet der Entwickler des EVGs konsequent Implementierungs-standards?
- Verwenden alle Drittanbieter konsequent Implementierungsstandards?
- Was gilt als 'Standard'?
- Legacy Code?
- Schlüssige Argumentation



Quelle: https://www.pexels.com/de-de/foto/laptop-buro-internet-technologie-177598/

Anforderungen 'Konfigurationsmanagement' - I

- 'Configuration Items' (CIs) gemäß ALC_CMS.5:
  - Der EVG selbst;
  - die Herstellernachweise (Evaluierungsdokumente);
  - die Anteile, die den EVG bilden;
  - die Implementierungsdarstellung;
  - Security Flaws + Resolution Status;
  - Entwicklungswerkzeuge und verwandte Informationen (z.B. Toolkonfigurationen)
- Alle Configuration Items müssen vom Konfigurationsmanagement-system verwaltet werden.
- Dafür können unterschiedliche Werkzeuge zum Einsatz kommen (z.B. Versionsverwaltung: GIT; Defect Tracking: JIRA)

Anforderungen 'Konfigurationsmanagement' - II

- Dokumentation und Benutzung des Konfigurationsmanagementsystems
- Zuzulassende EVGs müssen jeweils mit einer eindeutigen Referenz gelabelt sein.
- Das CM System muss alle CIs eindeutig identifizieren.
- Beschreibung wie die einzelnen CIs eindeutig identifiziert werden (typischerweise automatisch durch das CM Tool)
- Das CM System muss **automatisierte** Mechanismen zur Verfügung stellen, damit nur autorisierte Änderungen an CIs vergenommen werden können. -> Zugriffskontrolle
- Das CM System muss die Erstellung des EVGs mit automatischen Mechanismen unterstützen.
- <weitere Anforderungen an das CM System folgen>

Anforderungen 'Konfigurationsmanagement' - III

- Die CM-Dokumentation muss einen CM-Plan enthalten.
- Der CM-Plan muss beschreiben wie das CM-System benutzt wird, um zuzulassende EVGs zu entwickeln
- Der CM-Plan muss beschreiben, welche Prozeduren verwendet werden, um neue oder geänderte CIs zu akzeptieren, die Teil des TOEs sind. -> einschl. Akzeptanzprozeduren von Software Dritter!
- Das CM-System muss sicherstellen, dass die Person, die für die Akzeptanz eines CIs verantwortlich ist, nicht die Person ist, die das CI entwickelt hat.
- Die CM-Dokumentation muss rechtfertigen, dass die Akzeptanzprozeduren angemessene und geeignete Überprüfungen der Änderungen an allen CIs sicherstellen.
- Die CM-Dokumentation muss belegen, dass alle CIs (laut Definition in ALC_CMS) unter Kontrolle des CM Systems stehen (-> Screenshots)

Anforderungen 'Konfigurationsmanagement' - III

- Das CM System muss die CIs identifizieren, welche die TSF (Sicherheitsfunktionen zuzulassender EVGs) bilden.
- Das CM System muss die Auditierung aller Änderungen an zuzulassenden EVGs mit automatischen Mechanismen unterstützen, einschließlich der Information, wer die Änderung an welchem Tag und zu welcher Uhrzeit vorgenommen hat (-> logging).
- Das CM System muss in der Lage sein, die Version der Implementierungsdarstellung zu identifizieren, aus welcher der zuzulassende EVG generiert wurde (d.h. es soll vom CM Tool ermittelt werden können, aus welchen 'Sourcen' (inkl. Version) der zuzulassende EVG generiert wurde).
- Das CM System muss automatische Mechanismen zur Verfügung stellen, mit denen bei einer Änderung eines CIs die Identifikation aller anderen von der Änderung betroffenen CIs möglich ist.

➢ => Detailbetrachtung

17

Detailbetrachtung 'Auswirkung von Änderungen'

- Formal könnte man CIs z.B. als ST, Designdokumentation (gesamt), Source Code (gesamt), etc. ansehen. D.h. man könnte annehmen, dass es ausreichen würde, die Abhängigkeiten aus CC zu modellieren:
  - Bei einer Änderung am Security Target muss mich das CM Tool darauf hinweisen, dass ich auch das TOE Design, die Implementierung und die Tests auf Auswirkungen überprüfen muss.
- Erwartungshaltung Herstellerqualifizierung: Bei der Änderung/ Hinzufügen/Entfernen einer bestimmten Sicherheitsfunktionalität, sollen die Verweise möglichst konkret sein:
  - Z.B. Änderung der Beschreibung des Zufallszahlengenerators (RNG) im ST verweist auf das Design des RNGs im TOE Design, zur Implementierung des RNGs und zu den Tests des RNGs.
  - Das Tracing soll so zielgerichtet wie möglich umgesetzt werden. Das BSI unterstützt den Hersteller bei der Modellierung und Umsetzung.

18

Hohe Anforderungen

- **Warum sind die ALC Anforderungen bei der Herstellerqualifizierung so hoch?**
- Nach erfolgreicher Herstellerqualifizierung wird ein Großteil der Verantwortung für die Produktzulassung in die Hand des Herstellers gelegt.
- Da es sich um Produkte für die Verarbeitung von eingestuften Informationen handelt, soll die Prozesssicherheit die vollständige technische Evaluierung ersetzen.
- Der Aufwand für eine Herstellerqualifizierung ist in der Regel hoch, gibt dem Hersteller aber eine bessere Kontroller über den Zulassungsprozess.
- Nur mit dem BSI Zulassungsschema vertraute Hersteller kommen für eine Herstellerqualifizierung infrage.
- **Hersteller sollten sich bei Bedarf Unterstützung holen!**

19

Fragen?

Quelle: https://www.pexels.com/de-de/foto/mann-der-braune-jacke-tragt-und-grauen-laptop-benutzt-874242/

20

Vielen Dank für Aufmerksamkeit!

Was wir tun:

- **Zulassungsunterstützung**
- **Common Criteria Evaluierungen**
- **Beratung zu Evaluierung, Zulassung, Herstellerqualifizierung, Validierungen, etc.**
- **FIPS140-3 Validierungen (atsec US)**
- **…**

Dr. Michael Vogel
atsec information security GmbH
Steinstr. 70
81667 München
mvogel@atsec.com