Common Criteria voor evaluatie van beveiliging van IT-producten

Ir. P.W.M. Franken, ir. G.N. Nelemans en dr. ir. P.L. Overbeek

Hoe kan men weten welke beveiliging is te verwachten van een softwareproduct, en waar het vertrouwen in zo'n product op te baseren is? Onafhankelijke evaluaties door derden gebaseerd op duidelijke evaluatiecriteria vormen hier een goed antwoord. Gebaseerd op de ervaringen met onder andere het Orange Book en de ITSEC, is de Common Criteria for Information Technology Security Evaluation ontwikkeld.

Introductie

Het besef van het belang van informatiebeveiliging is groeiende, maar hoe kan men nu weten welke beveiliging is te verwachten van een softwareproduct, en waar het vertrouwen in zo'n product op te baseren is? Normaal gesproken zal men niet volledig willen vertrouwen op de ontwikkelaar, maar als gebruiker zelf alles gaan testen is ook ondoenlijk. Onafhankelijke evaluaties door derden gebaseerd op duidelijke evaluatiecriteria vormen hier een goed antwoord.

In het verleden hadden verschillende landen ieder hun eigen initiatieven ontplooid zoals de TCSEC in de Verenigde Staten, en ITSEC in Europa. Gebaseerd op die ervaring en de behoefte tot acceptatie door meerdere landen is door die landen een nieuwe beveiligingsevaluatiestandaard ontwikkeld, en aan ISO ter standaardisatie aangeboden: namelijk versie 2.0 van de Common Criteria ofwel in ISO-termen DIS 15408.

Een evaluatie van de beveiliging van een IT-product is een formeel onderzoek naar de beveiligingskwaliteiten van dat IT-product. Hierbij worden twee aspecten bekeken:
* Is de beveiligingsfunctionaliteit voldoende om de genoemde dreigingen af te dekken en regels af te dwingen.
* Biedt het product inderdaad de geclaimde beveiligingsfunctionaliteit.

De vraag of een product geschikt is voor een bepaalde omgeving of toepassing wordt niet geëvalueerd, maar blijft een zaak voor de gebruiker, te beantwoorden door bijvoorbeeld een risicoanalyse. Naast losse IT-producten worden ook IT-systemen geëvalueerd. Onder een systeem wordt in deze context verstaan een combinatie van verschillende IT-producten inclusief de operationele omgeving waarin deze producten actief zijn.

Er zijn drie doelgroepen die voordeel hebben bij beveiligingsevaluaties: gebruikers, product- en systeemontwikkelaars, en beoordelaars van systemen.

Gebruikers

Gebruikers van IT-producten willen weten of een geëvalueerd product aan hun beveiligingseisen voldoet. Bij een evaluatie worden de beveiligingseisen van een product nauwkeurig en volgens vaste regels vastgelegd. Een gebruiker kan daarom de resultaten van een evaluatie gebruiken om producten te selecteren of onderling te vergelijken. Ook kunnen de criteria worden gebruikt om de beveiligingseisen van de gebruikers vast te leggen. Bijvoorbeeld de beveiligingseisen waar een database met privacygevoelige gegevens aan zou moeten voldoen. Op basis van die vastlegging kunnen vervolgens producten worden gebouwd. Voor de specificatie van de beveiligingseisen kan een zogenaamd *Protection Profile* (PP) worden gebruikt. De inhoud van een PP wordt hierna behandeld.

Product- en systeemontwikkelaars.

Het voordeel voor een product- of systeemontwikkelaar van het hebben van een geëvalueerd product is afhankelijk van de situatie. Het product zal echter door een onafhankelijke partij zijn beoordeeld op vast omschreven functionaliteit. De voordelen zullen dus uiteenlopen van het hebben van:
* een kwaliteitsstempel op het product, een succesvolle evaluatie levert een certificaat over het product dat internationaal erkend wordt;
* een verbetering van de kwaliteit van het product. Door de onafhankelijke evaluatie zullen problemen eerder worden gevonden en kunnen worden verholpen. Zeker indien de evaluatie parallel loopt aan het ontwikkeltraject;
* een duidelijke en met andere producten vergelijkbare uitspraak over de functionaliteit van het product.

De bedoeling van evaluatiecriteria is ook om de ontwikkelaars van IT-producten te ondersteunen, vooral waar het gaat om producten die zullen worden geëvalueerd. De criteria stellen bepaalde eisen aan het ontwerptraject en de documenten en helpen daarmee de ontwikkelaars in het 'bouwen voor evaluatie' en het voorbereiden op de evaluatie. Een ander voordeel dat de ontwikkelaar heeft is dat de gebruikers hun behoeften via de eerdergenoemde PP's hebben opgeschreven. Een ontwikkelaar kan deze PP's gebruiken als een soort behoeftestelling van klanten die hij wellicht nog niet kent.

Beoordelaars van IT-producten of -systemen

De beoordelaar van een IT-product of -systeem kan het evaluatieresultaat bestuderen in plaats van alle activiteiten om de kwaliteit en geschiktheid van het product zelf uit te voeren. Systeemontwikkelaars of auditors kunnen dan sneller en effectiever tot oordelen over geschiktheid van het product komen.

Tussen bovengenoemde doelgroepen voor evaluatiecriteria bestaat een zeker spanningsveld. Een natuurlijke tegenstelling bestaat tussen de doelgroepen gebruikers en product- en systeemontwikkelaars. Daarnaast is er echter nog een 'doelgroep' voor de evaluatiecriteria, die van de beoordelaars (evaluators) zelf. De beoordelaar moet in een onafhankelijke positie ten opzichte van de hiervoor genoemde groepen gebruikers en product- en systeemontwikkelaars verkeren. Om dit verder af te dwingen is er onafhankelijk toezicht op de organisatie en werkwijze van de beoordelaar.

De criteria bieden dus een *meetlat* voor IT-beveiliging; een meetlat die kan worden gebruikt door zowel producenten als consumenten van (beveiligings)producten. De beoordelaar moet de meetlat aanleggen: objectief, herhaalbaar, controleerbaar en tegen redelijke kosten.

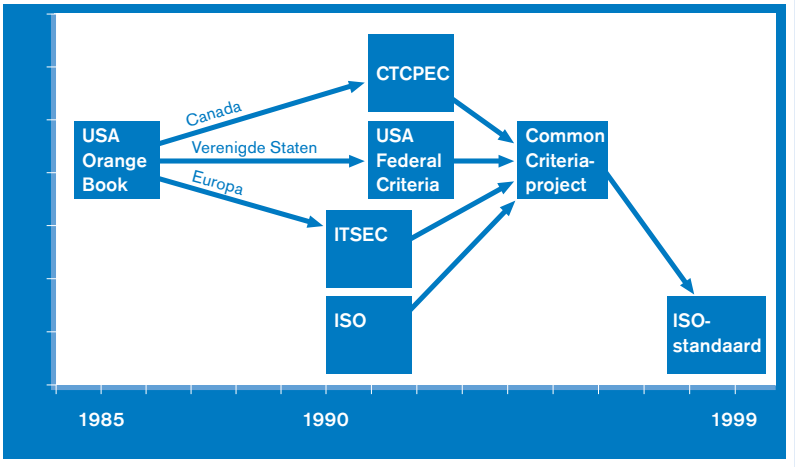
In dit artikel wordt het gebruik en de globale inhoud van evaluatiecriteria beschreven aan de hand van de *Common Criteria for Information Technology Security Evaluation versie 2.0* of kortweg CC ([CC98]).

De Common Criteria

De CC is ontwikkeld door Amerika, Canada, Frankrijk, Duitsland, Engeland en Nederland. De doelstelling is om de volgende generatie criteria voor de evaluatie van beveiliging in IT-producten te ontwikkelen en om wederzijdse erkenning van evaluaties tussen verschillende landen te verkrijgen. Op dit moment worden in Europa tegen de ITSEC geëvalueerde producten niet als zodanig erkend in Amerika. De CC moet een wereldstandaard worden, een ISO-standaard, zodat beveiligingsevaluaties onderling erkend worden en geen handelsbarrières creëren.

De CC is gebaseerd op de volgende 'oude' criteria: ITSEC, de TCSEC ofwel Orange Book, en de Canadese CTCPEC. Deze criteria zullen op den duur geheel verdwijnen ten gunste van de CC. Overigens blijven evaluaties tegen de 'oude' criteria gewoon geldig en kunnen voorlopig probleemloos evaluaties tegen bijvoorbeeld de ITSEC worden uitgevoerd. Tijdens de ontwikkeling van de CC zijn nauwe contacten met de ISO SC27 Werkgroep 3 'Evaluatiecriteria' onderhouden omdat de CC uiteindelijk een ISO-standaard moet worden. Momenteel is de CC-versie 2.0 al geaccepteerd als DIS 15408.

Figuur 1. Historie van evaluatiecriteria.



Het ontstaan van de Common Criteria

De historie van evaluatiecriteria begint onopvallend ergens in de jaren zeventig, toen de eerste ideeën rond het *Orange Book* ([TCS85]) ontstonden. Het Orange Book werd gepubliceerd in 1985 en was lange tijd de enige officiële set criteria. Als zodanig heeft het Orange Book een enorme stimulerende invloed gehad op beveiliging van IT-producten. Sinds 1990 is het 'criterialandschap' aanzienlijk veranderd. In Europa kwamen verschillende landen met eigen criteria uit. Deze zijn geharmoniseerd in wat uiteindelijk de ITSEC ([ITSE91]) is geworden. De ITSEC is in 1991 uitgekomen en vond binnen de doelgroep een brede erkenning in Europa. In ISO-verband werd in 1991 begonnen met de ontwikkeling van een internationale versie van de ITSEC. In Canada zag de CTCPEC ([CTC93]) in 1993 het licht en, eveneens in 1993, ontstond in de Verenigde Staten onder aanvoering van het NIST de eerste versie van de New Federal Criteria ([FC93]), als vervanger van het Orange Book. Deze historie van evaluatiecriteria is weergegeven in figuur 1.

Veranderingen op het gebied van beveiligingsevaluaties

De drijvende krachten en motieven voor beveiligingsevaluaties zijn aan het veranderen. Hiermee veranderen ook de wensen uit de markt op het gebied van evaluaties. Enkele van die veranderende factoren zijn:

* In het verleden werden beveiligingsevaluaties meestal uitgevoerd in opdracht van overheidsorganisaties. Steeds vaker vragen IT-producenten zelf om evaluatie van hun producten. De motivatie van een IT-producent (aanbieder) verschilt natuurlijk sterk van die van een overheidsorganisatie (doorgaans optredend namens de gebruikers binnen de overheid). Voor producenten spelen argumenten een rol als: toegang tot bepaalde markten voor geëvalueerde producten, productverbetering en de commerciële waarde van een certificaat (reclamewaarde). Bovendien is het voor een leverancier van belang dat het evaluatieproces synchroon kan lopen met de productontwikkeling en aansluit bij het normale ontwikkelproces en de opleveringstermijnen.
* De ontwikkelingen in de informatietechnologie (IT) gaan steeds sneller. Hiermee neemt de behoefte aan flexibiliteit in de criteria toe. Neem als voorbeeld de beveiligingsbehoeften in open, gedistribueerde systemen ([Over93]) zoals in gebruik in het Internet. De grenzen van wat wel en wat niet bij het systeem hoort, zijn niet op voorhand te trekken omdat deze systemen worden opgebouwd uit subsystemen. De vraag is dan: hoe kunnen subsystemen worden ontwikkeld (en geëvalueerd) die samen met andere *mogelijke* subsystemen een veilig systeem vormen?
* Ook de toepassing van de IT verandert. Hierdoor ontstaan nieuwe beveiligingsbehoeften, bijvoorbeeld op het terrein van de '*safety*'- en '*mission critical*'-systemen of de behoefte aan systemen met *Privacy Enhanced Technology*. Bij deze systemen ligt een zwaarder accent op beveiligingseisen als betrouwbaarheid en continuïteit.

* De markt vraagt om evaluaties die internationaal toepasbaar zijn. De reden hiervoor is dat de grootgebruikers van IT-producten zelf internationaal opereren.
* Eén van de hoofddoelen van evaluatiecriteria is de IT-beveiliging in producten te stimuleren en te verbeteren, in het belang van producenten en gebruikers. Dit is alleen binnen een beperkte financiële bandbreedte te bereiken. Of, anders gezegd, evaluaties moeten betaalbaar blijven.

Al deze factoren vragen om een bredere, wereldwijde benadering van beveiligingsevaluaties, hetgeen de belangrijkste reden is voor de ontwikkeling van de Common Criteria for Information Technology Security Evaluation.

Reikwijdte van de Common Criteria

De verwachtingen rond de CC zijn hooggespannen in de wereld van beveiligingsevaluaties. Met de CC wordt natuurlijk geen wondermiddel geboden, maar wat biedt de CC dan wel? Voorop staat dat de CC in de eerste plaats een harmonisatie en uitbreiding is van de bestaande evaluatiecriteria. Hierdoor kan verdere wildgroei worden voorkomen. Een afgeleid maar niet minder belangrijk doel is om evaluerende partijen bij elkaar te brengen en kennis te laten maken met elkaars evaluatiecultuur en werkmethoden.

Binnen het aandachtsgebied van de CC vallen:
* evaluatie van de beveiliging in IT-producten of -systemen;
* bescherming van informatie tegen menselijke of andere bedreigingen. De CC onderkent beveiligingsmaatregelen gericht op het bewaren van vertrouwelijkheid, integriteit, beschikbaarheid, privacy en controleerbaarheid van de informatie en de IT-middelen;
* technische aspecten van beveiliging;
* gebruik van en interfacing met cryptografische functies (niet de algoritmen zelf).

Buiten het aandachtsgebied van de CC vallen:
* evaluatie van niet-technische beveiliging. Organisatorische, procedurele en fysieke maatregelen vallen buiten de CC *tenzij* ze direct aan een technische maatregel verbonden zijn (bijvoorbeeld functiescheiding);
* evaluatie van in- en uitstralingsbeveiliging (Tempest);
* cryptografische algoritmen;
* de *methodologie* voor evaluaties. Om internationaal tot vergelijkbare evaluatieresultaten te komen is het ook nodig om gelijkwaardige evaluatiemethoden te gebruiken. Zo is er bij de Europese ITSEC een methodologie ontwikkeld, de ITSEM ([NGI95]), die door alle beoordelaars wordt gebruikt. De ontwikkeling van de 'Common ITSEM' is inmiddels in volle gang.

Inhoud van de CC

De CC is zowel geschikt voor IT-producten als -systemen; het is meestal niet nodig een onderscheid te maken. In de CC wordt dan ook de term *Target of Evaluation* (TOE) gebruikt. Met de TOE wordt het IT-product of -systeem met de bijbehorende gebruikers- en systeemdocumentatie verstaan dat het onderwerp van evaluatie is.

De CC bestaat uit drie delen. Eén deel (deel 1) beschrijft de algemene ideeën en principes en resultaten van een evaluatie. De andere twee delen gaan respectievelijk in op de *functionaliteit (Security Functional Requirements)* ofwel wat betekent beveiliging, en *zekerheid* (*Security Assurance Requirements*) ofwel hoe kunnen we vertrouwen verkrijgen dat het product daaraan voldoet.

Security Functional Requirements (functionaliteit)

De beveiligingseisen beschrijven de beveiligingsbehoeften van een TOE. De functies die deze eisen implementeren, zorgen samen voor het gewenste 'beveiligingsgedrag'. De CC (deel 2) bevat een catalogus met alle huidig bekende beveiligingsfuncties. Hieruit kan de beveiligingsfunctionaliteit worden geselecteerd die in een bepaalde situatie nodig is. Omdat de techniek niet stilstaat zal in de loop der tijd deze catalogus worden uitgebreid met nieuwe of verbeterde eisen. In de tussentijd kunnen Protection Profiles en Security Targets worden uitgebreid met functionaliteitseisen of zekerheidseisen welke niet in de CC worden genoemd. Hier zal later in het artikel iets verder op worden ingegaan.
De Security Functionaliteit is opgebouwd uit steeds fijnere elementen: allereerst de *Classes*, dan *Families*, en vervolgens de *Components*. De componenten zijn de onderdelen die in een Security Target en Protection Profile terugkomen. De indeling in classes en families is voornamelijk bedoeld om de functionaliteit te groeperen.

Tabel 1. Functionality Classes in de Common Criteria.

Functionality Class		Toelichting
FAU	**Security Audit**	Deze klasse bevat criteria voor de alarm- en incidentenaudit waaronder de registratie van en reactie op beveiligingsrelevante incidenten.
FCO	**Communication**	Bevat momenteel alleen criteria voor functies voor non-repudiation: bescherming tegen het ontkennen van datacommunicatie en communicatie tussen applicaties (onloochenbaarheid).
FCS	**Cryptographic Support**	Bevat criteria voor sleutelbeheer en cryptografische functies, al dan niet op basis van standaardalgoritmen.
FDP	**User Data Protection**	Bescherming van gebruikersdata: onder andere toegangsbeheersing, controle en authenticatie van informatiestromen alsmede import en export van data.
FIA	**Identification and Authentication**	Identificatie en authenticatie van personen en/of programma's die een gebruiker representeren.
FMT	**Security Management**	Management van beveiligingsfuncties en -attributen, management van beveiligingsrollen en bijbehorende rechten en plichten.
FPR	**Privacy**	Bescherming van de persoonlijke levenssfeer waaronder anonimiteit.
FPT	**Protection of the TOE Security Functions**	Bescherming van de beveiligingsfuncties van het systeem of product zelf.
FRU	**Resource Utilisation**	Gebruik en beheer van middelen: onder andere quota's en prioriteiten, maar ook foutbestendigheid.
FTA	**TOE Access**	Toegang tot de TOE (dit is het systeem of het product) zelf, waaronder het opzetten, blokkeren en afsluiten van sessies.
FTP	**Trusted Path/ Channels**	Deze klasse bevat criteria voor functies die een vertrouwd pad moeten bieden voor bescherming van de communicatie tussen de gebruiker en de TSF[1] of tussen TSF's onderling.

1) TSF staat voor Trusted Security Functions: de beveiligingsfuncties van de TOE.

Tabel 1 geeft de *Functionality Classes*. Dit is het hoogste niveau voor de functionaliteitsbeschrijving. De codering voor de Functionality Classes begint steeds met een 'F', gevolgd door twee letters uit de naam (F-AU, voor *F*unctionality Class '*Au*dit').

Security Assurance Requirements (zekerheid)

Assurance (zekerheid of verzekering) is de eigenschap van een TOE die de gebruiker het vertrouwen moet geven dat de TOE inderdaad veilig is ofwel daadwerkelijk de gewenste beveiligingsfunctionaliteit biedt. De zekerheid wordt onder andere ontleend aan de kennis van het ontwerp en de ontwikkeling van de TOE, in het licht van het bedoelde gebruik van de TOE. De vereiste maatregelen die het vertrouwen in de beveiliging moeten verzorgen, worden de Security Assurance Requirements genoemd. Een *Evaluation Assurance Level* representeert de diepgang waarmee de evaluatie wordt uitgevoerd. De termen Security Assurance Classes en Evaluation Assurance Level zullen hieronder nader worden toegelicht.

Tabel 2. Assurance Classes in de Common Criteria.

Assurance Class	Toelichting
ACM Configuration Management	Bevat voornamelijk criteria betreffende de kwaliteit van het configuratiebeheer tijdens de productontwikkeling.
ADO Delivery and Operation	Bevat criteria betreffende de veiligheid tijdens distributie naar de afnemers, installatie, systeemgeneratie, opstarten en overdracht.
ADV Development	Het beveiligingsmodel en de architectuur, de functionele specificatie, het globaal en gedetailleerd ontwerp alsmede de implementatie.
AGD Guidance documents	Criteria ter ondersteuning van gebruikers en beheerders betreffende het veilige gebruik van de TOE.
AMA Maintenance of Assurance	Criteria voor het onderhouden van het certificaat tijdens de levenscyclus van een product.
ALC Life cycle support	Criteria betreffende de veiligheid in de ontwikkelomgeving, het melden en verhelpen van fouten en storingen en de procedure rond de introductie van nieuwe versies.
ATE Tests	Criteria betreffende het testen van de TOE: welk gedeelte is getest, met welke diepgang en methode, en zijn er ook onafhankelijke tests uitgevoerd.
AVA Vulnerability Assessment	Criteria voor de analyse van zwakke punten, verborgen kanalen (covert channels), mogelijkheden voor misbruik en de sterkte van de gebruikte mechanismen.
APE Protection Profile Evaluation	Criteria betreffende de documentatie waar de evaluatie op kan worden gebaseerd. In de klasse APE zijn evaluatiecriteria voor de inhoud van Protection Profiles opgenomen.
ASE Security Target Evaluation	Criteria betreffende de documentatie waar de evaluatie op kan worden gebaseerd. In de klasse ASE zijn evaluatiecriteria voor de inhoud van Security Targets opgenomen.

Security Assurance Classes

Waarop kan het vertrouwen in een product worden gebaseerd? Hoe kan er in mindere of meerdere mate worden zekergesteld dat het product precies die functionaliteit biedt die benodigd is en dat er geen onverwachte gaten in de beveiliging zitten? De CC onderkent hiervoor verschillende groepen zekerheidsmaatregelen. De Assurance-eisen zijn opgebouwd uit steeds fijnere elementen: allereerst de *Classes*, dan *Families*, en vervolgens de *Components*. De Assurance Classes zijn opgenomen in tabel 2. De al genoemde Evaluation Assurance Levels zijn samengesteld uit deze componenten. Veel van de Assurance Classes zijn gerelateerd aan kwaliteitsaspecten en zijn ook terug te vinden in ISO 9000-stelsels. De codering voor de Assurance Classes begint steeds met een 'A', gevolgd door twee letters uit de naam (A-CM, voor *A*ssurance Class *C*onfiguration *M*anagement).

Evaluation Assurance Levels

Een Evaluation Assurance Level (zekerheidsniveau) is een samenstel van zekerheidsmaatregelen. Er is een zevental Evaluation Assurance Levels gedefinieerd: EAL1 tot en met EAL7. Elk niveau bouwt voort op het voorgaande niveau, dus EAL 5 heeft dezelfde zekerheidsmaatregelen als EAL 4 en een aantal meer. De Evaluation Assurance Levels zijn opgenomen in tabel 3.

Nieuw ten opzichte van oudere criteria is het EAL1-niveau dat een laag instapniveau biedt en meer mogelijkheden heeft voor leveranciersverklaringen (*vendor assurance*). Verder is er geen niveau zoals niveau D in de TCSEC of niveau E0 in de ITSEC, waarin gesteld wordt dat het product niet voldoet. In het Orange Book is *assurance* impliciet meegenomen, er bestaan geen aparte niveaus.

Evaluation Assurance Level	Beschrijving
EAL1	De functionaliteit is getest zoals bij een consumententest. De ontwikkelaar hoeft hierbij zo goed als niet betrokken te zijn.
EAL2	De functionaliteit is op structurele wijze getest.
EAL3	Volgens een vaste methodiek getest. Tevens een aantal eisen aan het ontwerp.
EAL4	Volgens een vaste methodiek getest. Ontwerp moet expliciet beveiligingsmodel omvatten.
EAL5	Semi-formeel beveiligingsmodel, ontwerp en specificatie.
EAL6	Als EAL5 maar met uitgebreidere evaluatiemethode voor testen van het model, het ontwerp en de specificatie.
EAL7	Het hoogste Evaluation Assurance Level vereist een formeel beveiligingsmodel, ontwerp en specificatie.

Tabel 3. Evaluation Assurance Levels in de Common Criteria.

De TOE en zijn beveiliging

Een TOE zal worden ontwikkeld in de verwachting dat het in de beveiligingsbehoefte voorziet van de beoogde gebruikers. Deze gebruikers zijn uiteraard zelf verantwoordelijk voor het onderkennen van hun beveiligingsbehoefte. De gebruikers kunnen deze behoefte bijvoorbeeld ontlenen aan een risicoanalyse maar deze behoefte kan ook worden ontleend aan een '*security baseline*'. Dat is een minimumniveau aan beveiliging dat binnen een organisatie of voor een specifieke toepassing als ondergrens wordt aangenomen. De Code voor Informatiebeveiliging ([CVI94]) geeft hiervoor een raamwerk. In

beide gevallen is er sprake van een specificatie van de bedreigingen voor de informatie en de informatieverwerkende omgeving, de zogenaamde bedreigingenomgeving. Ook een productontwikkelaar voert zo'n analyse uit voor zijn product, waarbij aannames worden gedaan over de bedreigingen in de beoogde verwerkingsomgeving. De bedreigingenomgeving wordt gebruikt om de beveiligingsdoelstelling voor de TOE op te stellen.

De beveiligingsdoelstellingen (*Security Objectives*) worden opgesteld naar aanleiding van de analyses van de omgeving van de TOE, het beoogde gebruik, de bedreigingen die de TOE aan moet kunnen en eventueel een referentie naar toepasbare externe richtlijnen (zoals wetten of beleid). De beveiligingsdoelstellingen worden vervolgens ingevuld door de hierboven beschreven Security Functional Requirements en Security Assurance Requirements. Voor dit proces, dat van iets abstracts als een bedreigingenomgeving naar een specifieke en geëvalueerde TOE leidt, gebruikt de CC een aantal bouwstenen. De CC kent als belangrijkste bouwstenen *Protection Profile* en *Security Target*. Deze bouwstenen zullen hierna worden toegelicht. Figuur 2 toont de samenhang tussen de bouwstenen.

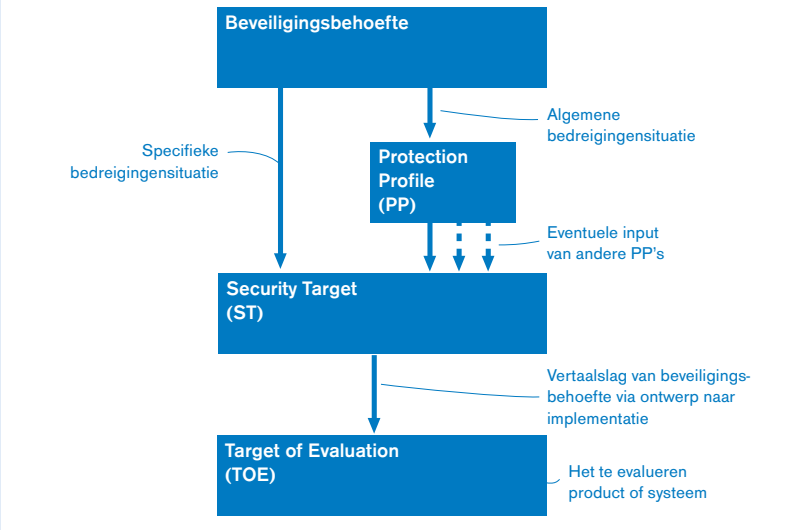
Hoewel de Protection Profiles en Security Targets de functionaliteitseisen en zekerheidseisen die in de Common Criteria worden genoemd, kunnen gebruiken, mag men ook andere eisen die niet in de CC staan opnemen. Hiermee kan de CC aan wijzigingen aan inzichten en behoeften voldoen en vormt een flexibele structuur. Deze eisen moeten natuurlijk wel aan dezelfde voorwaarden zoals objectief, evalueerbaar, enz. voldoen. Het gebruik van eisen van buiten de CC kan echter gevolgen hebben voor de acceptatie door anderen (ofwel internationale erkenning van het certificaat). Men zou zelfs een Protection Profile kunnen maken zonder een functionaliteits- of zekerheidseis uit de Common Criteria, zelfs Evaluation Assurance Levels zijn niet voorgeschreven. Wat men echter aan een dergelijk profiel heeft is de vraag.

Protection Profile

Een Protection Profile (PP, protectieprofiel) is een definitie van de beveiligingsbehoefte in een algemene bedreigingenomgeving. In de PP wordt onder andere beschreven wat de beoogde gebruikersomgeving is, welke bedreigingen daar gelden, wat de aannames over de omgeving zijn en welke beveiligingsdoelen in die omgeving worden gesteld (waarom bescherming nodig is). In het gedeelte van de PP met de eisen wordt vervolgens gedefinieerd welke beveiligingsfuncties nodig zijn om die doelen te bereiken (welke functionaliteit is nodig voor de bescherming die nodig is). Tevens wordt met een Evaluation Assurance Level aangegeven welke zekerheid wordt vereist dat de functionaliteit ook echt en continu wordt geboden.

Onderstaand worden enkele voorbeelden van mogelijke PP's weergegeven:

* De vroegere Orange Book-klassen C1, C2, B1, B2, B3 en A1 voor beveiliging van besturingssystemen zijn voorbeelden van PP's. Door deze klassen op te nemen ontstaat tevens een groeipad voor Amerikaanse (en Canadese) gebruikers.



Figuur 2. Bouwstenen van de Common Criteria.

* Hetzelfde als voor de Orange Book-klassen geldt voor de huidige ITSEC Predefined Functionality Classes.
* Momenteel wordt gewerkt aan een aantal voorbeeld-PP's, bijvoorbeeld voor *firewalls* en enkele besturingssystemen.
* Van standaarden zoals de GSS-APIS, de POSIX security interfaces en de ANSI-standaarden voor de bankwereld kunnen PP's worden ontwikkeld.

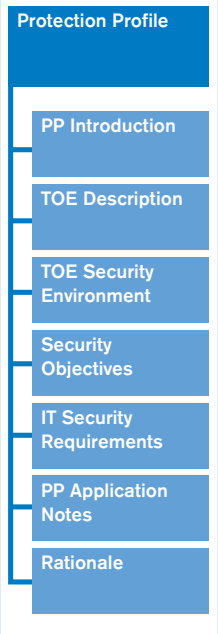
Er kunnen echter ook veel bredere PP's worden gemaakt. Hierbij kan worden gedacht aan profielen voor privacygevoelige applicaties, de medische omgeving, de *mission-* of *safety critical*-omgeving of voor het elektronisch zakendoen met EDI of elektronische post.

Het idee is dat een PP wordt ontwikkeld door een groep belanghebbenden, bijvoorbeeld een gebruikersgemeenschap of een groep aanbieders. Het PP wordt eerst geevalueerd en daarna via een register toegankelijk gemaakt voor alle gebruikers.

Inhoud van een Protection Profile

Figuur 3 toont de inhoud van een PP. De verschillende onderdelen van een PP worden hieronder beschreven:

* PP Introduction: bevat de *PP identification* waarmee iedere PP uniek te identificeren is en een korte beschrijving van het doel van deze PP in het *PP overview*.
* TOE Description: bevat een algemene beschrijving van de TOE zelf.
* TOE Security Environment bestaat uit de paragrafen *assumptions*, *threats* en *policies*:
  - De *assumptions*-paragraaf bevat de aannames over het beoogde gebruik en de toepassing van de TOE alsmede de aannames over de organisatorische, fysieke, personele en technische inbedding in de omgeving. Tevens bevat deze sectie aannames over de 'waarde' van de te beschermen informatie voor de organisatie en de beveiliging buiten de TOE.
  - *Threats* bevat de bedreigingen die de TOE het hoofd moet bieden. Dit onderdeel bevat een beschrijving van de bedreigingen in de omgeving zoals die hierboven is beschreven. In een bedreigingenscenario moet ook aandacht zijn voor (opzettelijke) aanvallen op de

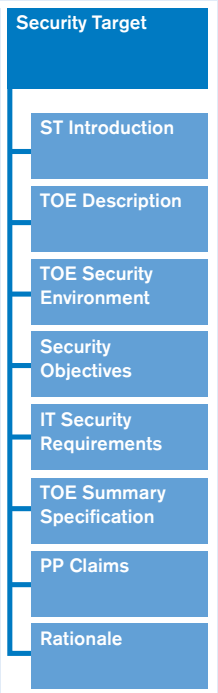


Figuur 3. Opbouw Protection Profile.

beveiliging en daarbij spelen onderstaande elementen een rol:
  - gelegenheid. De omgeving zal voor een groot deel bepalen of een aanvaller al dan niet in de gelegenheid is om een aanval op te zetten. Het tijdsaspect speelt hier ook een rol.
  - expertise, kennis. Welk kennisniveau heeft een aanvaller nodig en welke specifieke kennis van de TOE is benodigd om een succesvolle aanval uit te voeren.
  - hulpmiddelen en bronnen. Welke inspanning moet de aanvaller leveren en welke hulpmiddelen moeten de aanvaller daarbij ten dienste staan.
  - aanvalsmethode. Hoe zal de aanvaller proberen de beveiliging te compromitteren.
  - motivatie. Wat zouden de voordelen voor de aanvaller kunnen zijn, wat levert een succesvolle aanval eventueel op.
- In de *policies*-paragraaf worden de algemene beleidsuitgangspunten en eventuele wettelijke kaders met betrekking tot de TOE of de doelgroepen beschreven.

* Security Objectives: de beveiligingsdoelstelling van de TOE en de doelstellingen die in de omgeving van de TOE verwezenlijkt moeten zijn. De Security Objectives worden gebaseerd op de hierboven genoemde assumptions, threats en policies.
* IT Security Requirements: deze zijn opgebouwd uit de volgende twee gedeelten:
- TOE Security Requirements: specificatie van de requirements voor functionaliteit en zekerheid.
  - functionaliteit: functional requirements voor de TOE. De beschrijving van de functional requirements omvat de functionele eisen die aan de TOE gesteld worden (of aan de omgeving als de TOE daarop vertrouwt). Deze eisen zijn een selectie van de functionele componenten. In tegenstelling tot in de Security Target hoeven de componenten niet volledig gespecificeerd te zijn. Deze verdere specificatie kan aan de ontwikkelaars worden overgelaten.
  - zekerheid: Assurance Requirements voor de TOE, doorgaans in de vorm van een Evaluation Assurance Level, al dan niet met aanvullende Assurance Components.
- Security Requirements voor de IT-omgeving.

* PP Application Notes: aantekeningen met betrekking tot het gebruik van deze PP. Hieronder valt eventuele aanvullende informatie over de bouw, de evaluatie of het gebruik van de TOE. Er kan bijvoorbeeld worden verwezen naar gerelateerde PP's of een waarschuwing voor het beheer worden gegeven.
* Rationale: hierin wordt uitgelegd hoe de objectives tot stand zijn gekomen en hoe de geselecteerde requirements voorzien in de beveiligingsbehoefte.



Figuur 4. Opbouw Security Target.

Security Target

Een Security Target (ST) bevat de definitie van de beveiligingsfuncties en het Evaluation Assurance Level van een TOE. Een ST is qua opbouw vrijwel gelijk aan een PP, maar een ST is specifiek voor een bepaalde TOE en een bepaalde gebruikersomgeving. In de PP wordt nog veel aangenomen of verondersteld. In een ST is dat niet het geval: alle keuzen zijn gemaakt en alle components zijn geselecteerd. Op basis van de ST wordt de evaluatie uitgevoerd. De ST bevat dan ook een TOE-specifiek gedeelte.

Er zijn duidelijke relaties tussen Protection Profiles en Security Targets. Een producent kan een PP nemen en op basis daarvan een product ontwikkelen. De producent stelt dan zijn ST op waarin hij beschrijft hoe de PP in zijn product is geïmplementeerd. In het evaluatieproces wordt eerst onderzocht of de ST inderdaad overeenstemt met de PP (zoals de producent stelt) en vervolgens wordt het product tegen de ST geëvalueerd. Het is overigens niet noodzakelijk dat een ST wordt afgeleid uit één of meer PP's, een ST kan volledig zelfstandig worden gedefinieerd.

Inhoud van een Security Target

Figuur 4 toont de vaste inhoud van een ST. Zoals gezegd is het belangrijkste verschil met een PP dat een ST specifiek is voor een bepaalde TOE in een specifiek verondersteld omgeving en daarom een gedeelte bevat dat specifiek op de TOE betrekking heeft. Alleen de nog niet beschreven onderdelen worden hieronder beschreven:
* TOE summary specification: de ST bevat de eerste nadere verfijning van het requirementsniveau. Deze verfijning bestaat bijvoorbeeld uit de functionele specificatie voor de beveiliging en een definitie van de maatregelen voor assurance. De beschrijving moet eenduidig het verband tonen tussen de requirements (ofwel: de behoeften) en de functies (ofwel: de wijze waarop in de behoeften wordt voorzien). In de ST moet ook duidelijk worden gemaakt welke beveiligingsmechanismen en technieken worden gebruikt in de TOE en in welke functies deze worden ingezet.
* PP claims: waar nodig wordt een interpretatie en een verfijning voor de ST gegeven van de gebruikte PP's, bijvoorbeeld waar de PP's keuzemogelijkheden geven. Ook wordt al het nodige gespecificeerd waar in de PP nog aannames worden gedaan. Dit betreft onder andere de specificatie van de omgeving waarin de TOE zal worden gebruikt, de bedreigingen in die omgeving alsmede het gebruik en de toepassing van de TOE.

Gebruiksmogelijkheden van evaluatiecriteria

Met de komst van de Common Criteria is een belangrijke stap vooruit gezet op het gebied van evaluaties van IT-producten en -systemen. Er is een natuurlijk groeipad vanuit de huidige criteria (vooral ITSEC in Europa en Orange Book in de Verenigde Staten) naar de Common Criteria. Huidige en toekomstige investeringen in evaluaties tegen huidige criteria zijn beschermd daar deze evaluaties worden erkend in de Common Criteria. Eén van de belangrijkste winstpunten is dat er nu eindelijk een internationaal erkende basis voor evaluaties kan komen en daaropvolgend internationale erkenning van evaluatieresultaten. Een leverancier hoeft zijn product dan niet meer in bijvoorbeeld de Verenigde Staten én Europa te laten evalueren. Ook in de geest van de vrijhandel (WTO) is de komst van de Common Criteria een groot pluspunt.

Echter, het onderwerp 'beveiligingsevaluaties' is niet altijd los te zien van zaken als nationale veiligheid en landsbelang. Er is daarom meer nodig dan een goed stelsel criteria. Er is ook de politieke wil en durf nodig om tot een werkelijk internationale aanpak te komen. In Europa is dat proces reeds in volle gang.

De Common Criteria kent ook een aantal beperkingen: evaluatiecriteria zijn complex en het gebruik is zeker tijdsintensief te noemen. Doordat de Common Criteria een evenwicht zoekt tussen enerzijds flexibiliteit en anderzijds ondersteuning van de gebruiker is zij zeker voor een nieuwkomer niet direct toegankelijk.

Natuurlijk ontslaat het gebruik van de Common Criteria de gebruiker niet van de verplichting zelf het gezonde verstand te blijven gebruiken en keuzen te maken uit de in de Common Criteria gedefinieerde functies of zelf additionele functies te definiëren. De Common Criteria is een vehikel om de wensen en eisen te definiëren maar is geen 'magic bullet'.

De EDP-auditor en de Common Criteria

De vraag is op welke wijze de EDP-auditor gebruik kan maken van de Common Criteria voor zijn werkzaamheden. Hierbij kan de Common Criteria in eerste instantie worden gebruikt als Esperanto. Het geeft een groot aantal eisen en definities zodat misverstanden tussen verschillende partijen zoals klant en leverancier kunnen worden geminimaliseerd. Verder geeft het door het gebruik van Evaluation Assurance Levels een meetlat voor de kwaliteit van de beveiligingsfunctionaliteit. De toepasselijkheid van de functionaliteit kan natuurlijk niet in een meetlat worden uitgedrukt.

Bij het uitvoeren van een EDP-audit wordt onder andere onderzoek gedaan naar de beveiliging van applicaties of systemen. In termen van de Common Criteria zijn dit de TOE's. Het EDP-onderzoek betreft doorgaans zowel het systeem of de applicatie zelf als de wijze waarop de mensen in een organisatie ermee omspringen. Het EDP-onderzoek zou tijdens dit onderzoek geëvalueerde producten in de organisatie kunnen aantreffen. In plaats van het product door te lichten zou de Security Target als een statement over de werking van het product kunnen worden gebruikt en om te bepalen hoe de omgeving moet zijn ingericht.

Voor de beoordeling van een applicatie die of systeem dat niet is geëvalueerd, is de Common Criteria bij uitstek als inspiratiebron te gebruiken. De EDP-auditor kan hierbij met name gebruikmaken van de criteria die zijn gedefinieerd voor functionaliteit en zekerheid.

Ook voor het beoordelen van het gebruik van een TOE binnen een organisatie biedt de Common Criteria aanknopingspunten. Veelal stellen criteria bijvoorbeeld eisen aan documentatie, waarbij kan worden gedacht aan documentatie van de randvoorwaarden waarbinnen een geconstateerd beveiligingsniveau geldt. Deze randvoorwaarden zijn er in drie soorten: fysieke randvoorwaarden, applicatie- of systeemgerichte randvoorwaarden (bijvoorbeeld installatieopties) en organisatorische randvoorwaarden (bijvoorbeeld: scheiding van bevoegdheden eist maatregelen om te voorkomen dat men elkaar het eigen wachtwoord vertelt). De beoordeling van de organisatie als zodanig valt niet binnen het toepassingsgebied van de criteria, evenmin als de fysieke beveiliging.

De EDP-auditor zal ook namens een gebruikersgroep of een productontwikkelaar betrokken kunnen zijn bij de ontwikkeling van Protection Profiles.

Tot slot

De Common Criteria legt een goede basis om te komen tot een internationale set criteria voor de evaluatie van beveiliging van IT-producten en -systemen. Het voordeel hierbij is dat evaluaties tegen reeds bestaande criteria (zoals het Orange Book of de ITSEC) hun waarde niet verliezen daar ze door de Common Criteria worden meegenomen. Het erkennen van de Common Criteria als internationale basis voor evaluaties alsmede het internationaal erkennen van evaluatieresultaten tegen de Common Criteria is echter een proces dat enige tijd vergt daar elementen als marktacceptatie, nationale veiligheid en landsbelang een rol spelen.

Het nadeel van de huidige versie van de Common Criteria is dat de aanpak complex is, hetgeen de toegankelijkheid niet bevordert. De omvang van de criteria, bijna zevenhonderd bladzijden, speelt hierbij tevens een rol. Ook de theoretische insteek en het nogal formalistische taalgebruik bevorderen een snelle acceptatie niet. Desalniettemin omvat de Common Criteria vele beveiligingsfuncties die zeer nuttig en interessant zijn voor functionarissen die in mindere of meerdere mate betrokken zijn bij beveiliging. Met name voor EDP-auditors is het onderwerp 'evaluatiecriteria' (met in het bijzonder de Common Criteria) een onderwerp dat op de agenda hoort te staan.

Literatuur

[CC98]
Common Criteria for Information Technology Security Evaluation, (parts 1-3), versie 2.0, May 1998.

[CTC93]
Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), version 3.0, CSSC, CSE, januari 1993.

[CVI94]
Code voor Informatiebeveiliging – een leidraad voor beleid en implementatie, NNI / Ministerie van Economische Zaken, 1994.

[FC93]
Federal Criteria for Information Technology Security (FC), draft 1.0, NIST/NSA, januari 1993.

[ITSE91]
Information Technology Security Evaluation Criteria (ITSEC), versie 1.2, juni 1991.

[NGI95]
Evaluatiecriteria voor IT-beveiliging, P.L. Overbeek (red), NGI, 1995.

[Over93]
Towards secure open systems, P.L. Overbeek, 2e uitgave, juli 1993.

[TCS85]
Trusted Computer Systems Evaluation Criteria (TCSEC of Orange Book), US DoD 5200.28-STD, december 1985.