SWEDAC

Konsoliderad version av

Styrelsens för ackreditering och teknisk kontroll (SWEDAC) föreskrifter och allmänna råd (STAFS 2007:21) om organ som certifierar IT-säkerhet

Ändring införd: t.o.m. STAFS 2013:18

_____

Tillämpningsområde

1 § Dessa föreskrifter tillämpas på certifieringsorgan som är eller ansöker om att bli ackrediterade av SWEDAC för certifiering av IT-säkerhet hos IT-produkter, IT-system samt skyddsprofiler, Protection Profile (PP).

Föreskrifterna är ett komplement till SWEDAC:s föreskrifter och allmänna råd (STAFS 2010:10) om ackreditering samt SWEDAC:s föreskrifter och allmänna råd (STAFS 2013:5) om ackreditering av organ som certifierar produkter. (*STAFS 2013:18*).

Definitioner

2 § I dessa föreskrifter gäller de definitioner som anges i

1. standarden ISO/IEC 17065:2012 – *Certifieringsorgan – Allmänna krav vid certifiering av produkter (ISO/IEC 17065:2012)*, och
2. SIS Handbok 550 - *Terminologi för informationssäkerhet.*

Dessutom avses i dessa föreskrifter med

Evalueringsorganisation	Organisation eller organisationsenhet som utför utvärdering. Evalueringsorganisation kan även benämnas som evalueringsenhet eller evalueringsföretag.
Evalueringsrapport (Evaluation Technical Report)	Detaljerad teknisk rapport över genomförd utvärdering som lämnas av evalueringsorganisation till ett certifieringsorgan.
Certifieringsrapport (Certification/Validation Report)	Rapport vilken ges ut av det ackrediterade certifieringsorganet. Dokumentet summerar resultaten från utvärderingen och intygar

det sammanlagda resultatet. Det intygar även att evalueringsmetoder och procedurer har tillämpats på ett korrekt sätt. (*STAFS 2013:18)*.

Krav för ackreditering

3 § Enligt 6 § första stycket SWEDAC:s föreskrifter och allmänna råd (STAFS 2013:5) om ackreditering av organ som certifierar produkter skall den som ansöker om ackreditering visa att de kravspecifikationer mot vilka certifiering under ackreditering skall göras, samt tillämpningsdokument och dokument för tillverkningskontroll eller motsvarande, är entydiga och allmänt tillgängliga. Enligt andra stycket skall berörda intressenter ha getts tillfälle att delta i arbetet med att ta fram kravspecifikationerna. (*STAFS 2013:18*).

Allmänt råd till 3 §

Kravspecifikationerna kan exempelvis vara en utgåva av standarden ISO/IEC 15408 eller den internationella standarden Common Criteria (CC).(*STAFS 2013:18*).

4 § Ett ackrediterat certifieringsorgan skall ha vidtagit åtgärder som säkerställer att de hanterar informationssäkerhet på ett tillfredställande sätt. Detta innefattar även skydd av information som certifieringsorganet erhållit från kunder och leverantörer.

Allmänna råd till 4 §

Ett strukturerat arbetssätt för att säkerställa informationssäkerhetshantering finns exempelvis i standarden SS-ISO/IEC 27001:2006 – Ledningssystem för informationssäkerhet - Krav. Vald säkerhetsnivå bör avspegla utfallet ifrån genomförda riskanalyser. Riskanalyser bör vara genomförda utifrån kraven i gällande lagstiftning och ur ett affärsverksamhetsperspektiv.

Ovanstående grundas på de skyddsbehov som föreligger för att kunna hantera företagshemlig och annan skyddsvärd information (t.ex. angående utvärderingsuppdraget i sig) avseende utvärderad produkt/system.

Utformning av certifikat

5 § Ett utfärdat certfikat skall innehålla information i enlighet med *bilaga 1* till dessa föreskrifter.

Allmänna råd till 5 §
Certifieringsrapport bör innehålla rubriker och information avseende certifiering i enlighet med bilaga 2 till dessa föreskrifter.

Övrigt

6 § SWEDAC kan, i enskilda fall och om det finns särskilda skäl, medge undantag från tillämpningen av dessa föreskrifter.

Denna författning träder i kraft den 28 november 2007.

_____

STAFS 2013:18

Denna författning träder i kraft den 1 januari 2014. 2 § i äldre lydelse ska dock fortsätta gälla för de organ som med stöd av 2 punkten i övergångsbestämmelserna till styrelsens föreskrifter och allmänna råd (STAFS 2013:5) om ackreditering av organ som certifierar produkter tillämpar 3 § styrelsens föreskrifter och allmänna råd (STAFS 2007:12) om ackreditering av organ som certifierar produkter.

Bilaga 1

Utformning av certifikat

Certifikat relaterade till utvärdering av en IT-produkt

Ett certifikat, eller tillhörande rapport, utfärdat av ett ackrediterat certifieringsorgan som utgör resultat från utvärdering av en IT-produkt mot uppställda evalueringsmål, Security Targets (ST), skall innehålla nedanstående information:

1. tillverkare,
2. produktens namn och beteckning,
3. typ av produkt,
4. versionsnummer/utgåvenummer,
5. överensstämmelse med skyddsprofil (PP) om detta är tillämpligt,
6. använd IT-plattform vid utvärderingen, (frivillig)
7. namn på evalueringsorganisation, (frivillig)
8. namn på certifieringsorgan,
9. certifieringsrapportens beteckning,
10. datum då rapporten publicerades, och
11. evalueringsnivå.

Certifikatet skall även inkludera nedanstående uttalande:
”IT-produkten, vilken avses i detta certifikat, har utvärderats av en ackrediterad evalueringsorganisation genom att använda den metodik som beskrivs i [*ange aktuell kravspecifikation*] för att bedöma överensstämmelse.

Valideringen har genomförts i enlighet med kraven i SWEDAC:s föreskrifter och allmänna råd (STAFS 2007:21) om organ som certifierar IT-säkerhet och bygger på en sammanfattning av evalueringsorganisationens tekniska rapport. Certifikatet är inte ett generellt godkännande av IT-produkten från certifieringsorganet eller någon annan organisation som erkänner eller verkställer detta certifikat. Certifikatet avser endast den specifika produkten och version av denna i den konfiguration som utvärderats i enlighet med certifieringsrapporten. ”

Certifikat relaterade till utvärdering av en skyddsprofil (PP)

Ett certifikat utfärdat av ett ackrediterat certifieringsorgan som ett resultat från en utvärdering av en skyddsprofil skall innehålla nedanstående information:

1. organisation som utvecklat skyddsprofilen (PP),
1. skyddsprofilens (PP) namn/beteckning,
2. versionsnummer,
3. namn på evalueringsorganisation (frivillig),
4. namn på certifieringsorgan,
5. certifieringsrapportens beteckning,
6. publiceringsdatum, och
7. evalueringsnivå.

Certifikatet skall även inkludera nedanstående uttalande:
”Skyddsprofilen, vilken avses i detta certifikat, har utvärderats av en ackrediterad evalueringsorganisation genom att använda den metodik som beskrivs i [*ange aktuell kravspecifikation*] för att bedöma överensstämmelse.

Valideringen har genomförts i enlighet med kraven i SWEDAC:s föreskrifter och allmänna råd (STAFS 2007:21) om organ som certifierar IT-säkerhet och bygger på en sammanfattning av evalueringsorganisationens tekniska rapport. Certifikatet är

inte ett generellt godkännande av skyddsprofilen från certifieringsorganet eller någon annan organisation som erkänner eller verkställer detta certifikat. Certifikatet avser endast den specifika skyddsprofilen och version av denna i den konfiguration som utvärderats i enlighet med certifieringsrapporten. ”

Ovanstående bygger på texten som anges i Common Criteria Recognition Arrangement (CCRA) Annex J.

Bilaga 2

Innehållet i certifierings- eller evalueringsrapport

Certifierings- och evalueringsrapporten och dess betydelse

Evalueringsrapporten skrivs av evalueringsorganisationen för certifieringsorganet och utgör basen för certifieringsrapporten. Syftet med evalueringsrapporten är att redovisa alla utlåtande med motiveringar och avvikelser som resultat från utvärderingen, inkluderande fel funna vid utvecklingen av IT-produkten eller skyddsprofilen (PP) och utnyttjbara sårbarheter upptäckta vid utvärderingen. Evalueringsrapporten kan innehålla konfidentiell information.

Certifieringsrapporten är källan för detaljerad säkerhetsinformation om IT-produkten eller skyddsprofilen (PP) för intresserade parter. Målet är att ge praktisk information om IT-produkten eller skyddsprofilen (PP) till konsumenterna. Certifieringsrapporten behöver inte och skall inte innehålla konfidentiell information då den liksom evalueringsmål (ST), innehåller information som är nödvändig för konsumenten för att säkert utnyttja den utvärderade IT-produkten.

Kortfattad sammanfattning

Informationen i sammanfattningen bör ge en klar och tydlig överblick av utvärderingsresultatet. Målgruppen för sammanfattningen är utvecklare, konsumenter och utvärderare av säkra IT-produkter, skyddsprofiler (PP) och system. Sammanfattningen ger läsaren en grunduppfattning om IT-produkten eller skyddsprofilen (PP) och resultaten från utvärderingen. Vissa kundgrupper, (exempelvis ackrediteringsorgan, personer i ledande ställning) läser ofta enbart denna del av rapporten. Av detta skäl är det viktigt att all nyckelinformation från utvärderingen inkluderas i denna sektion. Sammanfattningen bör innehålla men inte begränsas till nedanstående:

1. namn på den utvärderade IT-produkten, förteckning över de av produktens komponenter vilka är del av utvärderingen, produktens version och namn på den organisation som utvecklat produkten,
2. namn på evalueringsorganisation,
3. datum då utvärderingen var avslutad, och
4. kort beskrivning av resultaten från utvärderingen innefattar
    a) assuranspaket,
    b) funktionalitet,
    c) summering av hot och organisatoriska säkerhetspolicys som tas om hand av den utvärderade IT-produkten,
    d) speciella krav på konfiguration,
    e) förutsättningar avseende användningsmiljön, och
    f) friskrivningsklausuler.

Identifiering och spårbarhet

Den utvärderade IT-produkten måste vara tydligt identifierbar. Programvarans versionsnummer, applicerbara uppdateringar av programvaran, hårdvarans versionsnummer och kringutrustning som bandstationer, printrar m.m. måste identifieras och registreras. Detta ger den rubricering och beskrivande information som är nödvändig för att entydigt identifiera den utvärderade IT-produkten. Fullständig identifiering av den utvärderade IT-produkten säkerställer att en fullständig och noggrann återgivning av IT-produkten kan återskapas för att användas vid framtida utvärderingar.

Säkerhetspolicy

Avsnittet om säkerhetspolicy avser beskrivning av IT-produktens säkerhetspolicy. Säkerhetspolicyn beskriver IT-produkten som en samling av säkerhetstjänster. Beskrivningen av säkerhetspolicyn innehåller policys eller regler vilka den utvärderade produkten måste uppfylla eller upprätthålla.

Förutsättningar och förtydligande av utvärderingens omfattning

Under denna rubrik beskriver man säkerhetsaspekterna på miljön/konfiguration i vilken IT-produkten förväntas att användas. Avsnittet ger en möjlighet att uttrycka och klargöra utvärderingens omfattning med hänsyn till de hot som inte omfattas av utvärderingen. Användare kan ta faktabaserade beslut avseende de risker som är associerade med användningen av IT-produkten. Användning, miljörelaterade förutsättningar och tydliggörande av utvärderingens omfattning med hänsyn till hot vilka inte räknas bör fastställas i detta avsnitt.

Förutsättningar för användning

För att skapa en utgångsnivå för utvärdering av IT-produkten måste förutsättningarna göras för produktens användande. Områden som korrekt installation och konfiguration, uppfyllda minimikrav på hårdvara m.m. måste förutsättas. Detta avsnitt dokumenterar alla förutsättningar för användning av IT- produkten under utvärderingen.

Miljörelaterade förutsättningar

För att skapa en utgångsnivå för utvärdering av produkten måste de miljörelaterade förutsättningarna klargöras. Detta avsnitt dokumenterar de miljörelaterade förutsättningarna för IT-produkten under utvärderingen.

Förtydligande av omfattningen

Detta avsnitt listar och beskriver hot mot IT-produkten vilka inte omfattas av den utvärderade produktens säkerhetsfunktioner. Det kan förekomma att kunder antar att vissa hot hanteras av IT-produkten medan produkten i realitet inte omfattar dessa hot. Det är av denna anledning som dessa undantagna hot listas som ett förtydligande. Det är dock opraktiskt att lista alla undantagna hot för en individuell produkt.

Arkitektur

Detta avsnitt beskriver IT-produkten och dess huvudsakliga komponenter på en övergripande nivå. Syftet med detta avsnitt är att beskriva hur de olika komponenterna förhåller sig till varandra.

Dokumentation

En komplett förteckning av den dokumentation vilken berör IT-produkten, som den utvecklande organisationen förser kunden med, finns i detta avsnitt. Det är viktigt att all relevant dokumentation är försedd med versionsnummer. Dokumentationen omfattar rekommendationer för användare, administration och installation. Administration och installationsrekommendationer kan vara i samma dokument.

Testning av IT-produkten

Avsnittet beskriver metodik, konfiguration, detaljnivå, resultat och de tester som gjorts av evalueringsorganisationen och den organisation som utvecklat IT-produkten.

Utvärderad konfiguration

Detta avsnitt dokumenterar IT-produktens konfiguration under utvärderingen. I normalfallet beskriver administration och installationsanvisningar nödvändig information för korrekt konfigurering av IT-produkten. IT-produkten kan vara möjlig att konfigurera på ett antal olika sätt beroende på den miljö i vilken den används eller påverkas av organisationens säkerhetspolicy.

Använda inställningar och detaljerad konfiguration med tillhörande motivering framgår i detta avsnitt. Detta avsnitt är av särskild vikt då det ger grundförutsättningarna för den utvärderade produktens installation.

Resultat från utvärderingen

Detta avsnitt beskriver de assuranskrav som IT-produkten uppfyller. En detaljerad beskrivning av dessa krav och detaljer runt hur produkten uppfyller vart och ett av dessa krav återfinns i evalueringsmålet (ST).

Utvärderarens kommentarer/Rekommendationer

Detta avsnitt används för att komplettera information om utvärderingsresultatet. Dessa kommentarer/rekommendationer kan visa på brister som upptäcktes under utvärderingen eller påtala funktioner vilka är särskilt användbara.

Bilagor

Bilagor används för att komplettera med ytterligare information som kan vara till nytta för läsaren men som inte logiskt passar in under någon av de fördefinierade rubrikerna (exempelvis fullständig beskrivning av säkerhetspolicyn).

Evalueringsmål (ST)

Evalueringsmålet (ST) måste inkluderas i certifierings- och evalueringsrapporten. Dock bör konfidentiell information eller annan teknisk information skyddas eller utelämnas (exempelvis information relaterad till patentskydd).

Terminologi

Terminologiavsnittet används för att öka rapportens läsbarhet genom förtydligande definitioner av förkortningar och termer vars betydelse inte är självklar.

Litteraturförteckning

Detta avsnitt listar all dokumentation som använts som källmaterial vid sammanställning av rapporten. Detta inkluderar men är inte begränsat till:

1. kriterium, metodik, dokumentation avseende regelverket,
2. teknisk referensdokumentation, och
3. dokumentation som använts vid utvärderingen från den organisation som utvecklat produkten.

För att säkerställa spårbarhet är det nödvändigt att all sådan dokumentation är identifierbart med utgåvedatum och versionsnummer.

Ovanstående bygger på texten som anges i Common Criteria Recognition Arrangement (CCRA) Annex I.