BESLUT

Datum	Diarienummer	Ärendetyp
2018-05-04	18FMV3960-1:1	3.1
	Dokumentnummer	Sida
	1.0	1(9)
Giltig t.o.m.	Upphäver	
t.v.		

Beslutande
Kristin Strömberg
Teknisk Direktör

Föredragande
Dan Olofsson
SPL Stab S&D

Designregel Härdning av IT-system, utgåva 1.0

Sammanfattning

Denna designregel reglerar användningen av rekommendationer för härdning (säkerhetskonfigurering) av IT-system ingående i de tekniska system för vilka FMV tar designansvar.

Designregeln ingår som en av flera designregler inom området IT-säkerhet och utgör designstyrande handlingsregler vid kravtolkning av de krav som Försvarsmakten ställer i *Beslut om krav på godkända säkerhetsfunktioner version 3.1(KSF v3.1)* kravklass *SFIS_HRD - Systemets komponenter ska härdas mot intrång.*

Innehåll

1 Inledning

1.1 Bakgrund

Härdning av IT-system är en förutsättning för att kunna uppfylla de krav som Försvarsmakten ställer i KSF 3.1, se ref [4], kravklass SFIS_HRD. Härdning innebär att i IT-systemet ingående operativsystem, inbyggda program (firmware), nätverkskomponenter, databaser och andra applikationer konfigureras på ett så säkert sätt som möjligt. Exempelvis kan åtkomsträttigheterna i systemet och dess ingående delar begränsas, möjliga attackvägar via osäkra funktioner i infrastrukturkomponenter och applikationer skäras av och exponering från externa enheter förhindras.

I många fall rådet en osäkerhet avseende vad som avses med kraven på härdning enligt KSF och kravtolkningen beror till stor del på de personliga erfarenheterna som finns i varje projekt respektive aktuell MUST-handläggares uppfattning. Detta medför att IT-systemen härdas utifrån olika rekommendationer baserat på personliga uppfattningar vilket försvårar möjligheterna till enhetlighet och effektivitet inom området.

1.2 Syfte

Det övergripande syftet med designregeln är att de tekniska system som FMV utövar tekniskt designansvar för ska bestå av IT-komponenter som tillsammans uppfyller Försvarsmaktens krav på härdning enligt KSF på ett så effektivt sätt som möjligt.

Designregeln skapar förutsättningar för:

1. att etablera en gemensam grund för samverkan mellan FMV och FM avseende kravtolkning och kravuppfyllnad inom området.
2. att möjliggöra för FMV och industrin att bygga upp kompetens inom området.
3. underlätta återbruk genom att IT-komponenter har härdats enligt samma rekommendationer.
4. att FMV kan ta designansvar för det tekniska systemet.
5. att det tekniska systemet kan ackrediteras inom FM.

1.3 Omfattning

Denna utgåva av designregeln definierar hur KSF v3.1 krav SFIS_HRD.2 ska tolkas inom FMV samt vilka rekommendationer som härdningen ska baseras på.

I denna utgåva definieras inte i vilken omfattning härdningsrekommendationerna ska implementeras, alltså hur mycket som ska härdas. Detta görs istället genom kravtolkning av övriga SFIS_HRD krav i varje enskilt fall.

1.4 Beroenden

Inga identifierade.

1.5 Avsteg

Avsteg från denna designregel får endast ske efter beslut av designansvarig. Begäran om avsteg framställs skriftligen och ställs till Teknisk Chef som efter samråd med KravF IT-säk fattar beslut avseende eventuellt avsteg.

1.6 Termer, definitioner och förkortningar

1.6.1 Termer och definitioner

Term	Definition	Källa	Kommentarer/ Anmärkningar
Härdning	Säkerhetskonfigurering av IT-system genom att det som inte behövs för IT-systemets definierade funktion ska vara begränsat avseende åtkomst, avstängt eller borttaget ur systemet.	allmänt vedertagen	
Tekniskt designansvar	Tekniskt designansvar utövas av Försvarets materielverk för alla produkter Försvarets materielverk levererar till Försvarsmakten	SAMO 2017 Annex A §A4	
Principen om minsta möjliga rättigheter (Least privilege)	För varje abstraktionslager i ett IT-system ska varje subjekt, alltså person, program eller process endast ska ha de rättigheter som behövs för att kunna utföra de handlingar och operationer som är legitima.	https://en.wikipedia.org/wiki/Principle_of_least_privilege	
IT-komponent	Del av IT-system	KSF v3.1	
IT-system	System med teknik som hanterar och utbyter information med omgivningen	KSF v3.1	

1.6.2 Förkortningar

Förk.	Fullständig benämning	Källa	Kommentarer / Anmärkningar
CIS	Center for Internet Security	www.cisecurity.org	
KSF	Krav på IT-säkerhetsförmågor hos IT-system	Beslut om krav på godkända säkerhetsfunktioner version 3.1 (KSF v3.1)	
KravF IT-säk	FMV kravföreträdare inom IT-säkerhetsområdet	15FMV6214-3:1, 2015-06-18	

2 Dokumentinformation

2.1 Dokumentändringsinformation

Datum	Utgåva	Beskrivning	Författare
2017-12-01	1.0	Första utgåvan	Christian Fenger-Krog

2.2 Giltighet

Gäller tills vidare.

2.3 Sekretessbedömning och ev. informationssäkerhetsklass

Detta dokument bedöms ej innehålla uppgifter som omfattas av sekretess.

2.4 Bilageförteckning

Ej tillämplig.

2.5 Referensdokument

Dokumenttitel	Dokumentbeteckning, datum	Utgåva nr
[1] Center for Internet Security härdningsrekommendationer, CIS benchmarks™	www.cisecurity.org/cis-benchmarks	
[2] White Paper. System Hardening Guidance for XenApp and XenDesktop.	December 1, 2016 (https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/system-hardening-for-xenapp-and-xendesktop.pdf)	1.1
[3] "Samråd" MUST Designregel Härdning	17FMV9847-1:1, 2017-11-30	

2.6 Styrande dokument

Dokumenttitel	Dokumentbeteckning, datum	Utgåva nr
[4] Beslut om krav på godkända säkerhetsfunktioner version 3.1 (KSF v3.1)	FM2014-5302:1 2014-06-13 14FMV11462-1, 2014-06-16	3.1
[5] SAMO 2017, Annex A	15FMV10173-4:1, 2016-12-21	

3 Diskussion

Härdning av IT-system är, tillsammans med regelbunden uppdatering av kända säkerhetsbrister med s.k. säkerhetspatchar en del av det breda grundläggande skyddet i ett IT-system.

Uppdatering av säkerhetsbrister med säkerhetspatchar åtgärdar kända brister kopplat till produktens specificerade funktion. Om och hur dessa brister kan utnyttjas av en angripare beror på hur produkten är utformad från leverantören samt hur den är konfigurerad i sin aktuella

instans. Säkerhetskonfigurering, eller härdning, utgår från principen att det som inte behövs för IT-systemets definierade funktion ska vara avstängt eller borttaget ur systemet.

En jämförelse med den fysiska världen skulle kunna vara se ett IT-system som en skyddsvärd byggnad med alldeles för många dörrar, alltså både sådana som behövs för den definierade verksamheten och sådana som är onödiga. Regelbundet upptäcks lås som inte fungerar som förväntat och det går därför inte att lita på att dörrarna faktiskt är låsta. Att uppdatera kända säkerhetbrister (patcha) är som att byta ut de låsen vi vet är trasiga mot nya. Att härda IT-systemet är jämförbart med att svetsa igen de dörrar som inte behövs så att även om låsen går sönder så finns ett skydd mot obehörigt intrång.

Härdning av IT-system baseras alltså till stor del på principen *Least privilege - Principen om minsta möjliga rättigheter*. För varje abstraktionslager i ett IT-system ska därför varje subjekt, alltså person, program eller process endast ska ha de rättigheter som behövs för att kunna utföra de handlingar och operationer som är legitima. Andra principer som omfattas är *Minimalize – Minimalisering* som innebär att mängden funktioner i systemet begränsas och *Defence in depth – Försvar på djupet* som innebär att det ska finnas säkerhetsfunktioner på olika nivåer i systemet; kommer man förbi en ska det finnas andra bakom.

För att härda IT-systemet på rätt sätt finns det en mängd olika rekommendationer från både tillverkare och andra aktörer på marknaden. Rekommendationer från tillverkare är begränsade till den aktuella produkten och ingår oftast i licenskostnaden. Kvaliteten på rekommendationerna kan vara svår att bedöma och varierar utifrån tillverkarens ambitionsnivå. Som alternativ finns rekommendationer från oberoende organisationer och dessa är oftast bredare och omfattar ett "paket" med de vanligaste systemdelarna. Dessa rekommendationer omfattas i många fall av licenskostnader alternativt kostnader för medlemskap i den aktuella organisationen.

Krav på härdning återfinns i KSF v3.1 kravklass SFIS_HRD. I denna klass finns krav SFIS_HRD.2 som lyder:

Ingående delar i systemet ska konfigureras enligt tillverkarens rekommendationer för säker konfiguration. Om sådana inte finns ska av IT-säkerhetsbranschen vedertagna rekommendationer för säker konfiguration av komponenttypen användas.

Vad *Tillverkarens rekommendationer* innebär är svårt att definiera i en designregel då det finns en mängd tillverkare och dessa har olika typer av rekommendationer. Då denna designregel ska ge en övergripande styrning inom området har SFIS_HRD.2 istället tolkats/omformulerats så att det ger förutsättningar för en sådan styrning. Förutsättningen är att *av IT-säkerhetsbranschen vedertagna rekommendationer* ska användas i första hand då det kan definieras oberoende av vilka produkter som ingår.

Designreglerna i kommande avsnitt utgår från detta synsätt. För att få förankring för Tolkningen/omformuleringen av krav SFIS_HRD.2 i KSF 3.1 samt innehållet i denna designregel har samråd inhämtats från MUST, se ref [3]

4 Designregel

4.1 Regel 1

4.1.1 Regeltillämpning

Krav SFIS_HRD.2 i KSF 3.1 ska tolkas enligt följande:
Ingående delar i systemet ska konfigureras i enlighet med av IT-säkerhetsbranschen vedertagna rekommendationer för säker konfiguration av komponenttypen. Om sådan inte finns ska tillverkarens rekommendationer för säker konfiguration användas.

4.1.2 Exempel

Detta innebär att kravet ska tolkas som att alla IT-system som ingår i tekniskt system som FMV tar tekniskt designansvar, se ref [5], för och som omfattas av KSF krav SFIS_HRD.2 i första hand ska härdas enligt de generella rekommendationer som definieras i denna designregel enligt Regel 2. Om det i dessa generella rekommendationer saknas underlag för härdning av relevant komponenttyp ska den aktuella tillverkarens härdningsrekommendationer användas enligt Regel 3.

4.2 Regel 2

4.2.1 Regeltillämpning

Med ”*av IT-säkerhetsbranschen vedertagna rekommendationer*” enligt Regel 1 avses CIS – Center for Internet Securitys härdningsrekommendationer s.k. CIS benchmarks™, se ref [1]

4.2.2 Exempel

Detta innebär att alla IT-system som ingår i tekniskt system som FMV tar designansvar för och som omfattas av KSF krav SFIS_HRD.2 i första hand ska härdas enligt relevanta CIS benchmarks.

Ett fiktivt IT-system innehåller programvarorna Windows, Red Hat Linux, Microsoft Office. Dessutom används Citrix XenDesktop. För Windows, Red Hat Linux och Microsoft Office finns CIS benchmarks för de aktuella versionerna. Dessa ska då användas för dessa programvaror.

4.3 Regel 3

4.3.1 Regeltillämpning

Om relevanta CIS benchmarks saknas för i IT-systemet ingående komponenttyper ska respektive tillverkares rekommendationer för säker konfiguration användas. Saknas även rekommendationer från tillverkaren ska eventuella andra relevanta rekommendationer användas. Vid tillämpning av Regel 3 ska samverkan avseende bedömning av olika alternativ ske med FMV kravföreträdare (KravF) IT-säk, ISD@fmv.se.

4.3.2 Exempel

För det fiktiva IT-systemet i 4.2.2 ovan saknas CIS benchmarks för Citrix XenDesktop. Istället ska då enligt Regel 1 tillverkarens rekommendationer användas, i detta exempel *System Hardening Guidance for XenApp and XenDesktop*, se ref [2]. Samverkan avseende denna kravtolkning sker först med FMV KravF IT-säk.

4.4 Regel 4

4.4.1 Regeltillämpning

Kravtolkningen av SFIS_HRD.1, SFIS_HRD.3, SFIS_HRD.4, SFIS_HRD.5, SFIS_HRD.6 och SFIS_HRD.7 ligger till grund för bedömningen avseende vilka av åtgärderna i de ovan definierade härdningsrekommendationerna som är relevanta för det aktuella systemet.

Krav på tillgänglighet behöver särskilt beaktas i denna bedömning då den kan påverkas både positivt och negativt av olika typer av härdningar.

4.4.2 Exempel

Om det fiktiva IT-systemet har höga krav på flexibilitet och ska behandla icke sekretessbelagd information i en omgivning med låg exponering kan en lägre nivå på härdningens omfattning bedömas rimlig jämfört med om det fiktiva IT-systemet inte behöver vara flexibelt, innehåller stor mängd sekretess och har en omgivning med större exponering.

5 Förutsättningar för designregelns användning

CIS benchmarks finns att tillgå via FMV:s centralorgan för standardisering och standarder inom civilt och militärt försvar, FSD. Se http://fsd.fmv.se

6 Planerad revidering och utveckling av designregel

Denna designregel kan framöver komma att kompletteras med styrning avseende till vilken nivå olika typer av IT-system ska härdas.

Det finns vid fastställandet av denna utgåva ännu ingen tidsplan för när nästa utgåva ska ges ut.

7 CCB ställningstagande

FMV CCB rekommenderar 2018-04-26 FMV Teknisk Direktör att fatta beslut om att fastställa designregel Härdning av IT-system, utgåva 1.0.

8 Beslut

Designregel Härdning av IT-system, utgåva 1.0 fastställs för tillämpning vid utveckling, anskaffning och vidmakthållande av IT-system som ingår i alla tekniska system för vilket FMV tar designansvar.

I beredningen av beslut har Stefan Lyander SPL Stab (Kvalitetschef), Jonas Persson SPL Armé (Teknisk Chef Mark), Jan Ericsson SPL Marin (Teknisk Chef Sjö), Axel Nilsson SPL Flyg (Teknisk Chef Flyg & Rymd), Lars Burström SPL LED (Teknisk Chef Led), Bo Persson SPL LOG, Mats Hallberg T&E TL, Jan Söderberg FSV Ledningsstöd samt Dan Olofsson SPL Stab S&D deltagit, den senare som föredragande.

Kristin Strömberg
Teknisk Direktör

Sändlista:
SPL
AL
T&E
FSV
M&I
Grip
FMV VHL Förvaltningsorganisationen (avsett för VHL.forbattringsforslag@fmv.se)

Arkiv

För kännedom
Försvarsmakten HKV (Avsett för Ulrika Evertsson Hansson, MUST)