Folkhälsomyndigheten

registrator@msb.se

Handläggare
Marie Hansson

Vårt ärendenummer
05259-2019
Ert ärendenummer
2019-14546

Datum
2020-02-26

Sida
1 (1)

Folkhälsomyndighetens remissyttrande över förslag till myndigheten för samhällsskydd och beredskaps föreskrifter om it-säkerhet för statliga myndigheter

Folkhälsomyndigheten har beretts tillfälle att inkomma med synpunkter angående rubricerade remiss och har följande att anföra:

Folkhälsomyndigheten tillstyrker de föreslagna föreskrifterna med tillhörande konsekvensutredning. Synpunkter på förslaget lämnas i bifogad excelfil.

Beslut om detta yttrande har fattats av generaldirektör Johan Carlson. I den slutliga handläggningen har avdelningscheferna Anders Tegnell, Britta Björkholm, Anna Bessö, Karin Tegmark-Wisell, Elisabeth Wall Bennett, chefsjuristen Bitte Bråstad samt enhetschefen Mats Eklund deltagit. Juristen Marie Hansson har varit föredragande.

Enligt Folkhälsomyndighetens beslut

Marie Hansson

Svar på remiss gällande förslag till: Myndigheten för samhällsskydd och beredskaps föreskrifter om it-säkerhet för statliga myndigheter

Om Excelarket
Genom att klicka på "välj" får du upp en för kolumnen anpassad rullista
Välj "övrigt" där inget annat alternativ är lämpligt.
Synpunkter på konsekvensutredningen lämnas från rad 115.

Svarande organisation:
Referens/diarienr: **2019-14546**

Synpunkter föreskrifter

Kap	§	Punkt	Synpunkter	Förslag till ändring	Övriga kommentarer
3	Övrigt	Övrigt	Kapitlet bör kompletteras med att säker utvecklingsmetodik samt säkra utvecklingsprocesser ska beaktas.		I de fall en myndighet bedriver egen utveckling men även krav som måste ställas på leverantörer.
4	Övrigt	Övrigt	Det bör förtydligas att nätverk- och infrastrukturkomponenter (brandväggar, switchar mm) är att betrakta som en produktionsmiljö eller del av en produktionsmiljö med högt ställda säkerhetskrav. Önskan är att det tydliggörs att till exempel en hypervisor inte kan ha lägre säkerhetskrav en den produktions-VM som körs ovanpå.		
4	Övrigt	Övrigt	Det bör förtydligas att lämplig uppdelning av ansvarsområden (”separation of duties”) ska beaktas. Bland annat avseende säkerhetsloggning och realtidsövervakning. De administratörer, vars administrativa aktiviteter ska kontrolleras och följas upp, får inte ha möjlighet att påverka de loggar som ska användas som underlag för dessa kontroller. De får inte heller kontrollera sig själva. Om inte myndigheten har möjlighet att tillse lämplig uppdelning av ansvarsområden så måste relaterade risker hanteras med andra kompenserande åtgärder.		

4	15	Övrigt	De konfidentialitetsrisker som hanteras genom kryptering introducerar nya möjliga tillgänglighetsrisker som måste hanteras. Det bör därför förtydligas att myndigheten måste ha rutiner för att hantera krypteringsnycklar. Det bör även förtydligas att myndigheterna måste beakta möjligheterna att vid behov byta ut krypteringslösningar (”Crypto-agility”). Vad avser krav på elektronisk signering (elektronisk underskrift) och verifiering av e-post så måste innebörden av detta även beaktas utifrån ett rättsligt perspektiv. MSB bör förtydliga syftet med kravet och kanske även förtydliga de juridiska (eIDAS) och säkerhetsadministrativa aspekterna vid val av certifikatutfärdare, riktlinjer för arkivering av signerade e-postmeddelanden, tidsstämplig mm. Om en myndighet skickar ett S/MIME-signerat e-postmeddelande till en medborgare, vilket inte är en uppenbart onödigt signatur då medborgaren bör kunna verifiera avsändaren på ett säkert sätt, så blir detta sannolikt att betrakta som en avancerad elektronisk underskrift (eller stämpel). Konsekvensutredningen har beaktat de tekniska aspekterna av att applicera en elektronisk signatur på ett e-		EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32014R0910&from=SV)
4	12	1	Det är otydlig vad skillnaden mellan "besluta" och "godkänna" innebär i kap.4 §13 och §14 är.		
4	31	1	Det är inte alltid praktiskt genomförbar för att skydda alla nätverksanslutna informationssystem med programvara som ger skydd mot skadlig kod. Här bör förtydligas att om det inte är möjligt att installera sådan programvara så måste andra lämpliga, dokumenterade, säkerhetsåtgärder vidtas för att hantera de risker som föreligger.		
4	Övrigt	Övrigt	Det bör förtydligas krav på rutiner vid återanvändning och avveckling av hårdvara. (Hårddiskar från produktion bör inte rakt av återanvändas i testmiljöer, trasiga hårddiskar från ett produktionssystem måste destrueras på ett säkert sätt mm.)		
Övrigt	Övrigt	Övrigt		Det bör kompletteras med krav på att myndigheter ansvarar för att kunna visa att dessa föreskrifter efterlevs.	Ner det gäller personuppgiftsbehandling kräver Dataskyddsförordningen lämplig säkerhet i förhållande till risk och att efterlevnad ska kunna påvisas (ansvarsskyldighet). Elektronisk behandling av personuppgifter i ett system kräver normalt en stödjande infrastruktur i form av nätverk, brandväggar, hypervisors mm. Om elektronisk personuppgiftsbehandling ska kunna genomföras i praktiken så har myndigheter redan idag ett krav att kunna visa att den typ av säkerhetsåtgärder som MSB föreslår efterlevs och är fungerande över tid. Det vore därför rimligt om MSBs föreskrifter inkluderade en liknande skrivelse avseende ansvarsskydlighet. Alternativt att MSB förtydligar att det redan finns lagstiftning som ställer denna typ av krav.

2	Övrigt	Övrigt	Förtydliga att dessa krav avseende IT-säkerhet även gäller i de fall myndigheten använder sig av en extern leverantör/molntjänst. För att i praktiken möta kraven på lämplig säkerhet i förhållande till risk och dessa föreslagna föreskrifter så räcker det inte att en myndighet reglerar skyldigheter i ett avtal. Myndigheten har ett ansvar att följa upp den externa partens säkerhetsarbete.		
Välj	Välj	Övrigt	De nya föreskrifterna om IT-säkerhet ställer skärpta krav på myndigheternas IT-säkerhet. Det kommer att innebära ett omfattande arbete för myndigheternas IT- verksamheter att anpassa sig till de nya kraven samt även kräva utökade resurser i form av personal, konsulter och produkter. De nya föreskrifterna träder i kraft den 1 juli 2020. Folkhälsomyndigheten anser att det är för kort tid för att myndigheterna ska hinna anpassa sig till de nya kraven. Mot denna bakgrund vore det önskvärt om ikraftträdandet av föreskrifterna senareläggs alternativt kompletteras med övergångsbestämmelser.		
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			

Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			

Behöver du fler rader att lämna synpunkter på:
Infoga så många rader du behöver. Du kan behöva kopiera listan.

Synpunkter Konsekvensutredningen

Rubrik	Synpunkter	Övriga kommentarer

Kap	**§**	**punkt**
Välj	Välj	Välj
Övrigt	Övrigt	Övrigt
1	1	1
2	2	2
3	3	3
4	4	4
5	5	5
	6	6
	7	7
	8	8
	9	9
	10	10
	11	11
	12	12
	13	
	14	
	15	
	16	
	17	
	18	
	19	
	20	
	21	
	22	
	23	
	24	
	25	
	26	
	27	
	28	
	29	
	30	
	31	
	32	
	33	
	34	