Myndigheten för samhällsskydd och beredskaps författningssamling

Utgivare: Anna Asp, Myndigheten för samhällsskydd och beredskap
ISSN 2000-1886

MSBFS
Remissutgåva
[Fyll i nr]
Utkom från trycket
den [Fyll i datum]

Förslag till föreskrifter om it-säkerhet för statliga myndigheter;

beslutade den xx mars 2020.

Myndigheten för samhällsskydd och beredskap föreskriver följande med stöd av 21 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

1 kap. Inledande bestämmelser

Tillämpningsområde

1 § Denna författning innehåller bestämmelser om sådana säkerhetskrav som avses i 19 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

2 § Om det i en annan författning finns någon bestämmelse som avviker från denna författning, gäller den bestämmelsen.

Begreppsförklaring

3 § I denna författning avses med

informationssystem	applikationer, tjänster eller andra komponenter som hanterar information. I begreppet ingår också nätverk och infrastruktur.
säkerhetsloggning	logg över säkerhetskritiska händelser.
redundans	tillstånd då mer än ett medel finns för att upprätthålla ett givet funktionssätt syftande till att säkerställa kontinuerlig drift och därigenom öka feltoleransen.
samhällsstörning	företeelser eller händelser som hotar samhällets skyddsvärden, såsom olyckor, kriser och krig.

2 kap. Hantering av säkerhet i informationssystem

Identifiering av ytterligare krav

1 § Myndigheten ska utifrån informationsklassning och riskbedömning, enligt 10 § Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:xx), identifiera behovet av att ställa ytterligare krav på informationssystem utöver de som ställs i dessa föreskrifter.

Ansvar, kompetens och resurser

2 § Myndigheten ska för varje informationssystem utse en ansvarig som ska säkerställa att ändamålsenliga och proportionella säkerhetsåtgärder införs, förvaltas, följs upp och utvärderas.

3 § Myndigheten ska ha en uppdaterad förteckning över vilken hård- och mjukvara som används i respektive informationssystem samt kopplingar inklusive dataflöden mellan olika informationssystem. Av förteckningen ska även framgå vilka informationssystem som behandlar information som bedöms ha behov av utökat skydd, eller i övrigt är centrala för myndighetens förmåga att utföra sitt uppdrag.

4 § Myndigheten ska för varje informationssystem dokumentera vilka kompetenser och resurser som krävs för att upprätthålla säkerheten över tid.

Bedömning av risk

5 § Myndigheten ska genomföra riskbedömningar enligt 10 § Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:xx), för enskilda informationssystem samt för myndighetens produktionsmiljö i sin helhet i syfte att identifiera och hantera hot och sårbarheter.

6 § Myndigheten ska följa den tekniska utvecklingen i syfte att identifiera hot mot och sårbarheter i myndighetens informationssystem.

3 kap. Utveckling och anskaffning av informationssystem

Kravställning och kontroll

1 § Myndigheten ska inför utveckling och anskaffning av informationssystem identifiera och fastställa de krav på säkerhet som behövs för att uppnå avsedd funktionalitet.

2 § Vid identifiering och fastställande av krav på säkerhet ska minst följande, utifrån behov och omfattning, beaktas

1. segmenterad nätverksarkitektur,
2. autentisering och behörighetskontroll,
3. kryptering vid lagring och kommunikation,
4. säkerhetsloggning och tillhörande analys,
5. övervakning av informationssystem inklusive systemsäkerhetsfunktioner,
6. robust, korrekt och spårbar tid,
7. skydd mot skadlig kod,
8. säkerhetskopiering,
9. redundans,
10. säkerhetstester och granskning,
11. utbildning och utbildningsmiljö, samt
12. åtgärder som möjliggör kontrollerad avveckling, avställning och arkivering.

3 § Myndigheten ska dokumentera vilka säkerhetsåtgärder som valts för att möta fastställda krav.

4 § Myndigheten ska innan driftsättning och inför förändring som kan påverka säkerheten i informationssystem kontrollera att ställda krav på säkerhet uppfylls. Kontrollen ska ske genom säkerhetstester och granskning. I de fall säkerhetsbrister kvarstår ska dessa riskbedömas och hanteras innan driftsättning eller förändring.

5 § Myndigheten ska innan driftsättning och inför förändring kontrollera att det för berört informationssystem finns korrekt och tillräcklig dokumentation avseende arkitektur, ingående komponenter, konfiguration, dataflöden och övrig relevant systeminformation. Dokumentationen ska ge tillräckligt stöd för strukturerad och säker drift samt förvaltning.

6 § Myndigheten ska bedöma och hantera behovet av säkra och tillförlitliga informationssystem för intern och extern informationsspridning vid incidenter och under samhällsstörningar.

Säkra utvecklings- och testmiljöer

7 § Myndighetens utvecklings- och testmiljö ska vara separerade från produktionsmiljön samt uppfylla de krav på säkerhet som behövs för att uppnå avsedd funktionalitet.

4 kap. Drift och förvaltning av informationssystem

Separera, segmentera och filtrera

1 § Myndigheten ska, utifrån informationsklassning och riskbedömning, enligt 10 § Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:xx), tillämpa separation i produktionsmiljön. För att förhindra spridning av it-incidenter ska, om det inte är uppenbart onödigt, följande placeras i separata nätverkssegment

1. klienter för användare,
2. klienter för administration,
3. servrar,
4. centrala systemsäkerhetsfunktioner i form av behörighetskontrollsystem, säkerhetsloggning, filtrering och liknande,
5. centrala stödfunktioner i form av skrivare, scanner och liknande,
6. trådlösa nätverk,
7. gästnätverk,
8. externt åtkomliga tjänster,
9. informationssystem som sammankopplas med extern leverantör,
10. industriella informations- och styrsystem, samt
11. system som innehåller sårbarheter som inte kan hanteras.

2 § Myndigheten ska genom filtrering säkerställa att endast nödvändiga dataflöden förekommer mellan olika nätverkssegment.

Behörigheter, identiteter och autentisering

3 § Myndigheten ska säkerställa att samtliga identiteter i myndighetens produktionsmiljö är unika. Alla identiteter ska innan de kopplas till en individ eller ett informationssystem godkännas och dokumenteras.

4 § En och samma identitet får inte användas vid åtkomst till utvecklings- och testmiljö respektive produktionsmiljö.

5 § Myndigheten ska utforma sin behörighetshantering på ett sådant sätt att varje identitet inte har mer åtkomst till information än vad arbetsuppgiften kräver.

6 § Identiteter som ger systemadministrativ behörighet får endast användas för systemadministration och ska tilldelas restriktivt. En identitet

med systemadministrativ behörighet får endast ges åtkomst till en begränsad del av produktionsmiljön.

7 § Behörigheter ska vara tidsbegränsade. Myndigheten ska vid behov, dock minst en gång per år kontrollera att utdelade behörigheter är korrekta.

8 § Myndigheten ska identifiera och hantera behov av separata katalogtjänster för behörigheter. Katalogtjänster för externt åtkomliga informationssystem samt utvecklings- och testmiljö ska separeras från andra katalogtjänster.

9 § Flerfaktorsautentisering ska användas vid

1. åtkomst till produktionsmiljön via externt nätverk,
2. systemadministrativ åtkomst, samt
3. åtkomst till informationssystem som hanterar uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400).

10 § Vid övrig åtkomst till myndighetens informationssystem ska behovet av flerfaktorsautentisering övervägas.

Lösenord och koder

11 § Myndigheten ska ha interna regler för lösenord och koder som innehåller krav på längd och komplexitet samt hur och när lösenord och koder ska distribueras och bytas. Efterlevnaden av de interna reglerna ska, om det inte är uppenbart onödigt, stödjas av tekniska system för hantering av lösenord och koder.

Kryptering

12 § Myndigheten ska utifrån informationsklassning och riskbedömning, enligt 10 § Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:xx), besluta vilka krypteringslösningar som får användas vid kommunikation respektive lagring av myndighetens information.

13 § Myndigheten ska utifrån informationsklassning och riskbedömning, enligt 10 § Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:xx), godkänna vilka krypteringslösningar som får användas vid kommunikation respektive lagring av information.

14 § Myndigheten ska använda kryptering för att skydda säkerhetsloggar, lösenord och koder mot förändring och obehörig åtkomst vid kommunikation och lagring.

15 § Myndigheten ska, om det inte är uppenbart onödigt, införa

1. elektronisk signering och kryptering av e-post,
2. verifiering av signerad e-post, och

3. Domain Name System Security Extensions (DNSSEC).

Säkerhetskonfigurering av hårdvara och mjukvara

16 § Innan informationssystem tas i drift ska myndigheten genomföra säkerhetskonfigurering genom att kontrollera att funktioner som inte behövs stängs av eller tas bort, byta ut förinställda lösenord samt anpassa förinställda konfigurationer till identifierat behov av funktionalitet och säkerhet.

Ändringshantering och uppdatering av programvara

17 § Myndigheten ska ha interna regler för ändringshantering som säkerställer att alla förändringar i produktionsmiljön utförs på ett strukturerat och spårbart sätt. Risker för störningar i produktionsmiljön ska identifieras och hanteras innan förändringar genomförs.

18 § Myndigheten ska endast tillåta att på förhand godkända programvaror installeras och exekveras i myndighetens produktionsmiljö.

19 § Myndigheten ska ha interna regler för uppdatering av programvara som säkerställer att samtliga programvaror i produktionsmiljön uppdateras till senaste version utan onödigt dröjsmål. Föreligger hinder för uppdatering ska detta riskbedömas och hanteras.

20 § Myndigheten ska utan onödigt dröjsmål byta ut programvaror som inte längre uppdateras av leverantören. Risker relaterade till att använda programvara som inte längre uppdateras av leverantören ska riskbedömas och hanteras.

21 § Myndigheten ska snarast möjligt införa säkerhetsuppdateringar som åtgärdar sårbarheter. Föreligger hinder för uppdatering ska detta riskbedömas och hanteras.

Robust, korrekt och spårbar tid

22 § Myndigheten ska använda tidstjänsten Swedish Distributed Time Service eller motsvarande, för att säkerställa robust och korrekt tid spårbar till den svenska tillämpningen av koordinerad universell tid, UTC(SP).

Säkerhetskopiering

23 § Myndigheten ska säkerhetskopiera information som behövs för myndighetens förmåga att utföra sitt uppdrag minst en gång per dygn.

24 § När säkerhetskopiering genomförs ska myndigheten, utifrån identifierat behov, dock minst en gång per år, kontrollera att uppgifterna på säkerhetskopiorna går att återskapa inom för myndigheten godtagbar tidsperiod.

25 § Säkerhetskopior ska förvaras på ett betryggande sätt skilda från produktionsmiljön.

Säkerhetsloggning och realtidsövervakning

26 § Myndigheten ska dokumentera vilka uppgifter som ska loggas och var loggningsuppgifter ska hämtas. Säkerhetsloggningen ska skapa spårbarhet och minst omfatta

1. användares och systemadministratörers åtkomst till uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400),
2. systemadministratörers förändringar av konfigurationer och systemsäkerhetsfunktioner, samt
3. förändringar i åtkomsträttigheter.

27 § I centrala systemsäkerhetsfunktioner ska säkerhetsloggning utformas för att möjliggöra utredning av intrång, tekniska fel och brister i säkerheten.

28 § Myndigheten ska säkerställa jämförbarhet mellan loggar genom användning av myndighetens tidstjänst.

29 § Myndigheten ska analysera innehållet i säkerhetsloggarna i syfte att upptäcka och hantera avvikelser och incidenter.

30 § Myndigheten ska bedöma behovet av teknisk realtidsövervakning i informationssystem.

Skydd mot skadlig kod

31 § Myndigheten ska skydda nätverksanslutna informationssystem med programvara som ger skydd mot skadlig kod.

Särskilda it-utrymmen

32 § Myndighetens ska placera servrar för informationssystem i särskilda it-utrymmen. Informationssystem som ska skapa redundans ska inte placeras i samma it-utrymme. Behovet av att placera ytterligare infrastruktur för informationshantering i särskilda it-utrymmen ska identifieras och hanteras.

33 § Myndighetens särskilda it-utrymmen ska skyddas mot obehörig åtkomst genom tillräckligt skalskydd. Tillträde till särskilda it-utrymmen ska registreras på individnivå och dokumentationen ska sparas i minst 5 år.

34 § Myndigheten ska identifiera och hantera behovet av övervakning och larm i myndighetens särskilda it-utrymmen.

5 kap. Särskilt för bevakningsansvariga myndigheter

1 § Bevakningsansvariga myndigheter enligt bilaga till förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap ska, om det inte är uppenbart onödigt, använda flerfaktorsautentisering för åtkomst till informationssystem som behandlar information som, enligt 10 § Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:xx), har bedömts ha behov av utökat skydd, eller i övrigt är centrala för myndighetens förmåga att utföra sitt uppdrag.

2 § Bevakningsansvariga myndigheter ska minst en gång per kvartal kontrollera funktionaliteten hos informationssystem som ska användas för informationsspridning under samhällsstörningar.

Denna författning träder i kraft den 1 juli 2020.