Myndigheten för civilt försvars författningssamling

Utgivare: Anna Asp
ISSN 3119-2394

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

Myndigheten för civilt försvars föreskrifter och allmänna råd om säkerhetsrevision och säkerhetsskanning;

beslutade den [Fyll i datum].

Myndigheten för civilt försvar föreskriver[1] följande med stöd av 38 § 7 p. cybersäkerhetsförordningen (2025:1507).

Allmänna råd har en annan juridisk status än föreskrifter. De är inte tvingande. Deras funktion är att förtydliga innebörden i lag, förordning och föreskrifter och att ge generella rekommendationer om deras tillämpning.

1 kap. Inledande bestämmelser

Tillämpningsområde

1 § Dessa föreskrifter och allmänna råd innehåller bestämmelser om sådan säkerhetsrevision och säkerhetsskanning som avses i 3 kap. 5–7 §§ cybersäkerhetslagen (2025:1506).

Ordförklaringar

2 § Uttryck i dessa föreskrifter och allmänna råd har samma betydelse som i cybersäkerhetslagen.

3 § I dessa föreskrifter och allmänna råd avses med

digital miljö	den samlade mängden system som verksamhetsutövaren använder för att bedriva verksamhet. Består av produktionsmiljö och i tillämpliga

[1] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148, i den ursprungliga lydelsen (NIS2-direktivet).

	fall, utvecklings-, test- respektive utbildningsmiljö,
system	nätverks- och informationssystem enligt 1 kap. 2 § p. 16 cybersäkerhetslagen,
säkerhetsrevision	granskning av cybersäkerheten i system hos verksamhetsutövaren i syfte att bedöma om de säkerhetsåtgärder som har vidtagits för att skydda systemen och för att säkerställa efterlevnad av kraven i cybersäkerhetslagen med tillhörande reglering är ändamålsenliga och effektiva. Revisionen ska kunna visa på nivån av cybersäkerhet i systemen,
säkerhetsskanning	skanning av system för att upptäcka sårbarheter eller osäker konfiguration,
viktig samhällsfunktion	en samhällsfunktion som är nödvändig för samhällets grundläggande behov, värden eller säkerhet.

2 kap. Säkerhetsrevision

Tillsynsmyndighetens val av oberoende organ för säkerhetsrevision

1 § Det oberoende organ som anlitas för att utföra en säkerhetsrevision ska vara en juridisk person med expertkunskap utifrån uppdragets utformning och vid behov ha kunskap om den verksamhet som granskningen avser.

Allmänna råd

Vid tillsynsmyndighetens bedömning av det oberoende organets lämplighet för uppdraget bör det oberoende organets egen nivå av cybersäkerhet, tid och resurser för att kunna utföra uppdraget beaktas.

Vid bedömning av expertkunskap utifrån uppdragets utformning kan det oberoende organets kunskaper inom cybersäkerhet, granskningsmetodik och säkerhetsrevision beaktas.

2 § Tillsynsmyndigheten ska säkerställa att det oberoende organ som anlitas för att utföra en säkerhetsrevision ska genomföra uppdraget med opartiskhet, självständighet och objektivitet.

Vidare ska tillsynsmyndigheten säkerställa att utföraren

1. inte ingår sekretessavtal eller andra motsvarande överenskommelser, som inskränker tillsynsmyndighetens tillgång till relevant information, med verksamhetsutövaren som är föremål för granskning, och
2. inte nyttjar information som erhållits i samband med säkerhetsrevisionen för annat än genomförande av den aktuella säkerhetsrevisionen.

Allmänna råd

Tillsynsmyndigheten bör inte anlita ett oberoende organ som har affärsrelationer, rådgivningsuppdrag eller andra beroendeförhållanden till den verksamhetsutövare som är föremål för granskning. Tillsynsmyndigheten bör begära att det oberoende organet informerar tillsynsmyndigheten om sådan intressekonflikt uppstår under uppdraget.

3 § Tillsynsmyndigheten ska i samband med att en säkerhetsrevision inleds upplysa verksamhetsutövaren om

1. uppdragets omfattning, och
2. möjligheten att informera tillsynsmyndigheten om eventuella brister i det oberoende organets genomförande av säkerhetsrevisionen.

Det oberoende organets genomförande av säkerhetsrevision

4 § Tillsynsmyndigheten ska säkerställa att det oberoende organ som anlitas för att utföra en säkerhetsrevsion dokumenterar avvikelser och ger tillsynsmyndigheten resultatet av genomförd revision. I en säkerhetsrevision ingår att kontrollera både utformningen och tillämpningen av säkerhetsåtgärder.

Allmänna råd

En säkerhetsrevision bör omfatta både tekniska och icke-tekniska moment, såsom granskning av en verksamhetsutövarens interna digitala miljö, interna regler och arbetssätt, avtal eller överenskommelse om utkontraktering samt övrig dokumentation.

5 § En säkerhetsrevision ska utformas på ett sådant sätt att den inte vållar större kostnad eller olägenhet för verksamhetsutövaren än vad som är nödvändigt.

6 § Säkerhetsrevisionen ska genomföras enligt en granskningsmetodik som möjliggör en systematisk och riskbaserad granskning av verksamhetsutövarens organisatoriska, tekniska, driftrelaterade och fysiska säkerhetsåtgärder. Den granskningsmetodik som används ska dokumenteras.

Allmänna råd

Det oberoende organet bör som stöd vid utformning av metodiken och genomförande av säkerhetsrevisionen använda nedan etablerade standarder eller motsvarande såsom

- Bedömning av överensstämmelse – Krav på organ som reviderar och certifierar ledningssystem (ISO/IEC 17021-1:2015),
- Bedömning av överensstämmelse - Krav på verksamhet inom olika typer av kontrollorgan (ISO/IEC 17020:2012),
- Informationsteknik - Säkerhetstekniker - Vägledning för revision av ledningssystem för informationssäkerhet (ISO/IEC 27007:2020),
- International standard on assurance engagements 3000 (revised) assurance engagements other than audits or reviews of historical financial information (Effective for assurance reports dated on or after December 15, 2015),
- Vägledning för revision av ledningssystem (ISO 19011:2018).

Det oberoende organet bör i sin granskning av organisatoriska, tekniska, driftrelaterade och fysiska säkerhetsåtgärder utgå ifrån standarder som ger stöd för den specifika revisionen.

7 § Innan en säkerhetsrevision inleds ska tillsynsmyndigheten ha godkänt revisionens omfattning och tillvägagångssätt.

8 § Säkerhetsrevisionen ska inkludera följande moment

1. granskning av dokumentation,
2. intervjuer med berörd personal,
3. verifiering av organisatoriska säkerhetsåtgärder, och
4. tekniska kontroller av system.

Momenten i punkterna 2–4 ska, om inte särskilda skäl talar emot, utföras på plats hos verksamhetsutövaren.

9 § Om en sårbarhet, som inte tidigare har publicerats, upptäcks i verksamhetsutövarens digitala miljö vid genomförandet av en säkerhetsrevision ska tillsynsmyndigheten säkerställa att det oberoende organet utan dröjsmål informerar verksamhetsutövaren och tillsynsmyndigheten om sårbarheten.

10 § Efter genomförd säkerhetsrevision ska en skriftlig granskningsrapport och övrig relevant dokumentation överlämnas till tillsynsmyndigheten.

Information om identifierade brister och sårbarheter ska hanteras så att uppgifterna inte röjs för obehöriga.

3 kap. Säkerhetsskanning

Omfattning och utförare

1 § En säkerhetsskanning ska genomföras i den omfattning som är nödvändig för tillsynen och endast avse system som verksamhetsutövaren har rådighet över.

2 § En säkerhetsskanning får endast genomföras i den del av den digitala miljön som är nödvändig för tillsynen.

Allmänna råd

Säkerhetskanningar bör ske med automatiserade verktyg i den mån det är lämpligt i förhållande till syftet med åtgärden.

3 § Vid en säkerhetsskanning ska lämpliga åtgärder vidtas för att minska negativ inverkan på funktionaliteten i systemen och övriga negativa konsekvenser för verksamhetsutövaren.

4 § En säkerhetsskanning ska utföras av en tillsynsmyndighet eller av en av tillsynsmyndigheten anlitad extern aktör.

5 § Den externa aktören som anlitas för att utföra en säkerhetsskanning ska vara en juridisk person. Den juridiska personen ska tillhandahålla för uppdraget lämplig personal med för uppdraget nödvändig specialistkompetens.

Riskbaserat urval och olika typer av säkerhetsskanning

6 § Innan en tillsynsmyndighet beslutar om att genomföra en säkerhetsskanning ska den säkerställa att

1. urval av verksamhetsutövare sker utifrån en riskbedömning,
2. valet av vilka system som ska skannas sker utifrån en riskbedömning, och
3. de metoder som ska användas är lämpliga i förhållande till de identifierade riskerna och de system som ska skannas.

Allmänna råd

Verksamhetens betydelse för viktiga samhällsfunktioner bör beaktas vid urvalet. En riskbedömning rörande valet av vilka system som ska skannas bör göras utifrån

- om systemet är sektorskritiskt,
- tidigare incidenter eller rapporterade sårbarheter,
- exponering mot internet, och
- teknisk riskprofil, såsom kända sårbara system.

---

7 § Tillsynsmyndigheten ska beakta systemens betydelse för verksamheten vid val av metod vid utförande av en säkerhetsskanning.

Vid betydande risk för störningar ska alternativa metoder övervägas samt om säkerhetsskanning alls ska genomföras.

Allmänna råd

Innan en säkerhetsskanning inleds bör tillsynsmyndigheten tillsammans med verksamhetsutövaren

- fastställa om systemen är sektorskritiska,
- bedöma risken för driftpåverkan,
- planera genomförandet så att belastningen på systemen minimeras,
- ha en plan för att kunna avbryta säkerhetsskanningen, och
- bedöma behovet av att säkerställa förmåga att återställa systemen som kan påverkas negativt.

Informationsskyldighet

8 § Tillsynsmyndigheten eller den externa aktören som anlitats för säkerhetsskanning ska utan dröjsmål underrätta verksamhetsutövaren om identifierade brister och sårbarheter.

Om en sårbarhet, som inte tidigare har publicerats, upptäcks vid genomförandet av en säkerhetsskanning ska tillsynsmyndigheten säkerställa att den externa aktören utan dröjsmål informerar verksamhetsutövaren och tillsynsmyndigheten om sårbarheten.

Denna författning träder i kraft [Klicka och skriv tidsangivelse].

Myndigheten för civilt försvar

MIKAEL FRISELL

Ida Sahlin
Avdelningen för cybersäkerhet och samhällsviktiga kommunikationer

Beställningsadress:
Norstedts Juridik, 106 47 Stockholm
Telefon: 08-657 95 00
E-post: order@forlagssystem.se
Webbadress: www.nj.se/offentligapublikationer
Beställningsnummer: