Myndigheten för civilt försvars författningssamling

Utgivare: Anna Asp
ISSN 3119-2394

MCFFS 2026:11
Utkom från trycket
den 18 juni 2026

Myndigheten för civilt försvars föreskrifter och allmänna råd om säkerhetsåtgärder och ledningens utbildning för väsentliga och viktiga verksamhetsutövare;

beslutade den 15 juni 2026.

Myndigheten för civilt försvar föreskriver[1] följande med stöd av 38 § p. 5 och 39 § p. 1 cybersäkerhetsförordningen (2025:1507) och beslutar följande allmänna råd.

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 säkerhetsåtgärder och utbildning enligt 2 kap. 3 och 4 §§ cybersäkerhetslagen (2025:1506).

För verksamhetsutövare som uteslutande bedriver sektorsverksamhet inom digital infrastruktur, digitala leverantörer, förvaltning av IKT-tjänster (mellan företag), post- och budtjänster samt rymden gäller endast kraven på ledningens utbildning om säkerhetsåtgärder i 2 kap. 1 § i denna författning.

2 § Om annan författning innehåller bestämmelser som ställer högre krav än kraven i dessa föreskrifter tillämpas den bestämmelsen.

[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 (NIS 2-direktivet).

Ordförklaringar

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

4 § I dessa föreskrifter och allmänna råd avses med

Begrepp	**Betydelse**
digital miljö	den samlade mängden system som verksamhetsutövaren använder för att bedriva intern verksamhet och tillhandahålla externa tjänster. Består av produktionsmiljö och, i tillämpliga fall, utvecklings-, test- respektive utbildningsmiljö,
information i behov av utökat skydd	information som på grund av externa krav kräver en viss nivå av skydd avseende konfidentialitet, riktighet inklusive autenticitet, eller tillgänglighet alternativt information som verksamhetsutövaren vid värdering bedömer ha behov av motsvarande nivå av skydd,
it-segment	ett nätverkssegment som är inrättat för andra system än sådana system som placeras i ot-segment,
ot-segment	ett nätverkssegment som är inrättat för cyberfysiska system,
personal	egna anställda och externt kontrakterade personer inklusive anlitade uppdragstagare,
produktionsmiljö	de system i den digitala miljön som används för att bedriva verksamhet förutom de system som används för verksamhet i utvecklings- test- och utbildningsmiljö. Består av it-segment och ot-segment,
redundant funktion	två eller flera, identiska eller olika, funktioner som oberoende av varandra uppfyller samma syfte,
sektorskritiskt system	ett system som är nödvändigt för att kunna bedriva intern verksamhet eller tillhandahålla externa tjänster inom sektorsverksamhet,

Begrepp	Betydelse
sektorsverksamhet	sådan verksamhet som omfattas av cybersäkerhetslagen,
system	nätverks- och informationssystem enligt 1 kap. 2 § p. 16 cybersäkerhetslagen,
systematiskt och riskbaserat arbete med cybersäkerhet	arbete som bedrivs med stöd av interna regler och arbetssätt för att omhänderta identifierade risker när verksamhetsutövaren inriktar, utformar, inför, upprätthåller, övervakar, kontrollerar och utvecklar sin cybersäkerhet,
särskilda it- och ot-utrymmen	en lokal med tillträdesbegränsning eller ett låst skåp som är särskilt utformat för att skydda hårdvara i syfte att säkerställa systemens funktionalitet och nivå av fysiskt skydd,
viktig samhällsfunktion	en samhällsfunktion som är nödvändig för samhällets grundläggande behov, värden eller säkerhet.

2 kap. Ledningens utbildning om säkerhetsåtgärder

1 § Utbildningen ska ge ledningen den kunskap och kompetens som krävs för att kunna fastställa mål och inriktning för verksamhetsutövarens cybersäkerhet, bedöma vilka säkerhetsåtgärder som verksamhetsutövaren behöver genomföra för att upprätthålla en lämplig nivå av cybersäkerhet utifrån identifierade risker samt övervaka genomförandet av säkerhetsåtgärderna.

Allmänna råd

Ledningens utbildning bör omfatta

- ledningens roll i ett systematiskt och riskbaserat cybersäkerhetsarbete inklusive relevant terminologi och reglering,
- vilken betydelse cybersäkerheten hos verksamhetsutövaren har för att upprätthålla sektorsverksamhet och viktiga samhällsfunktioner,
- riskhantering och övervakning som ett stöd för att leda och styra arbetet med cybersäkerhet, samt
- för ledningen relevanta interna regler, arbetssätt och stöd.

3 kap. Organisatoriska säkerhetsåtgärder

Systematiskt och riskbaserat arbete med cybersäkerhet

1 § Verksamhetsutövaren ska bedriva ett systematiskt och riskbaserat cybersäkerhetsarbete utifrån ett allriskperspektiv. I arbetet ska även ingå att

1. identifiera och analysera externa krav, interna behov och risker avseende cybersäkerhet,
2. utifrån externa krav, interna behov och identifierade risker utforma och införa säkerhetsåtgärder,
3. följa upp och utvärdera identifierade risker och införda säkerhetsåtgärder, samt
4. vid behov förbättra införda säkerhetsåtgärder.

Arbetet ska integreras med befintligt sätt att leda och styra organisationen.

2 § Verksamhetsutövaren ska identifiera och hantera behovet av att använda relevanta standarder i cybersäkerhetsarbetet.

Allmänna råd

Som stöd för arbetet bör följande eller motsvarande standarder användas:

- Svensk standard SS-ISO/IEC 27001:2022 Informationssäkerhet – cybersäkerhet och integritetsskydd – Ledningssystem för informationssäkerhet – Krav.
- Svensk standard SS-EN ISO/IEC 27002:2022 Informationssäkerhet – cybersäkerhet och integritetsskydd – Informationssäkerhetsåtgärder.

Interna regler och arbetssätt

3 § Verksamhetsutövaren ska fastställa de interna regler och arbetssätt som behövs för att vidta lämpliga och proportionella säkerhetsåtgärder utifrån externa krav, interna behov och identifierade risker avseende cybersäkerhet.

Interna regler och arbetssätt ska utgå från verksamhetsutövarens fastställda mål och inriktning för cybersäkerheten samt uppdateras vid behov. De interna reglerna och arbetssätten ska i relevanta delar kommuniceras till berörd personal samt vid behov kompletteras med stöd för hur de interna reglerna och arbetssätten ska användas.

Verksamhetsutövaren ska identifiera och hantera behovet av att dokumentera och spara information som behövs för uppföljning och utvärdering respektive för tillsynsändamål.

Allmänna råd

Av interna regler och arbetssätt bör följande framgå

- vilken säkerhetsåtgärd som avses,
- vilka roller som berörs,
- fastställandedatum samt vilken roll eller ansvarsområden som ansvarar för att dokumentationen hålls uppdaterad,
- beskrivning av vad som ska göras, av vilken roll eller ansvarsområden, hur och när,
- vilka beslut som ska fattas, av vilken roll eller ansvarsområden och när, samt
- hur efterlevnaden av interna regler och arbetssätt ska dokumenteras.

Verksamhetsutövaren bör, för att kunna bedöma ändamålsenlighet och effektivitet av cybersäkerheten vid uppföljning och utvärdering respektive tillsyn, spara interna regler och arbetssätt samt relevant dokumentation över tillämpningen.

Bedömningen av vilken information som ska dokumenteras och hur länge dokumentationen ska sparas bör utgå från de behov som verksamhetsutövaren har avseende uppföljning och utvärdering.

För tillsynsändamål bör beslut, analyser, bedömningar, planer och resultat av uppföljning dokumenteras och sparas.

Roller, ansvarsområden och befogenheter

4 § För att verksamhetsutövaren ska kunna vidta lämpliga och proportionella säkerhetsåtgärder ska ledningen godkänna och övervaka genomförandet av säkerhetsåtgärder genom att säkerställa att

1. det finns fastställda mål och inriktning för cybersäkerheten,
2. ledningens uppgifter i cybersäkerhetsarbetet är tydliggjorda,
3. det finns resurser för att bedriva ett systematiskt och riskbaserat cybersäkerhetsarbete,
4. de roller och ansvarsområden som cybersäkerhetsarbetet kräver har tillräckliga befogenheter och resurser för att utföra tilldelade uppgifter, samt
5. ledningen blir informerad om genomförandet av säkerhetsåtgärderna och verksamhetsutövarens nivå av cybersäkerhet vid behov men minst en gång per år.

Allmänna råd

I ledningens uppgifter i arbetet med cybersäkerhet bör ingå att fastställa

- kriterier för riskacceptans,
- prioriteringsordning för återställning av verksamheter, och
- vilka system som är sektorskritiska.

5 § Verksamhetsutövaren ska utse roller eller ansvarsområden för samordning av cybersäkerhetsarbetet (samordnare), för säkerheten i informationsbehandling i system (informationsägare) och för säkerheten i system (systemägare).

All informationsbehandling i system ska ha en utsedd informationsägare och alla system ska ha en utsedd systemägare.

6 § Samordnaren ska ha i uppgift att samordna det systematiska och riskbaserade arbetet med cybersäkerhet och utvärdera nivån av cybersäkerhet i förhållande till externa krav, interna behov och identifierade risker. Samordnaren ska säkerställa att de underlag som ledningen behöver för att godkänna och övervaka genomförandet av säkerhetsåtgärder sammanställs.

Allmänna råd

Samordnaren bör vid utvärderingen av nivån av cybersäkerhet utgå från

- fastställda mål och inriktning,
- informationsklassningar och riskanalyser samt aktuella åtgärdsplaner,
- uppföljningar och utvärderingar av införda säkerhetsåtgärder,
- information om inträffade incidenter och tillbud samt genomförda grundorsaksanalyser,
- utvärderingar av cybersäkerheten hos leverantörer och i digitala leveranskedjor, samt
- interna och externa revisioner samt genomförd tillsyn.

I sammanställningen av underlag till ledningen bör ingå

- uppgifter om hot och risker som bedöms som allvarliga för verksamhetsutövarens cybersäkerhet,
- uppgifter om bristande cybersäkerhet hos leverantörer och i digitala leveranskedjor,
- resultatet av intern och extern revision samt genomförd tillsyn,
- samordnarens utvärdering av verksamhetsutövarens nivå av cybersäkerhet, samt
- identifierade hinder för att uppnå ledningens mål och inriktning för cybersäkerheten och föreslagna åtgärder för att undanröja sådana hinder.

7 § Informationsägaren ska, för den informationsbehandling som denne ansvarar för, ha i uppgift att säkerställa att informationen är värderad och att risker analyserats samt utifrån detta bedöma vilken nivå av skydd informationen behöver ha avseende konfidentialitet, riktighet inklusive autenticitet, och tillgänglighet.

Informationsägaren ska informera berörd systemägare om identifierad nivå av skydd för informationen samt vad som är acceptabla tider för otillgänglighet och bristande funktionalitet för informationsbehandlingen.

Informationsägaren ska säkerställa att lämpliga och proportionella säkerhetsåtgärder är vidtagna för informationsbehandlingen.

8 § Systemägaren ska, för de system som denne ansvarar för, ha i uppgift att säkerställa att risker analyserats och att informationsägarens identifierade nivå av skydd uppnås i berörda system.

Systemägaren ska informera berörda informationsägare om brister i systemens cybersäkerhet som påverkar informationsbehandlingen. Systemägaren ska säkerställa att systemen, under hela deras livslängd, är skyddade med lämpliga och proportionella säkerhetsåtgärder.

Personalsäkerhet

9 § För att förebygga att personal orsakar incidenter på grund av olämplighet eller okunskap ska verksamhetsutövaren fastställa

1. vilka kontroller som ska genomföras i samband med rekrytering och anlitande av personal med utgångspunkt i vilken information och vilka system de ska få tillgång till,
2. vilka kontroller som ska genomföras av personal vid förändrad åtkomst till information och system, samt
3. vilka utbildningar, övningar och andra informationsinsatser avseende cybersäkerhet som personal ska genomföra innan och under anställning eller uppdrag.

Allmänna råd

För att vid rekrytering och anlitande av personal kunna bedöma deras lämplighet och kunskap om cybersäkerhet bör identitetskontroll, intervju, kontakt med referenser samt verifiering av akademiska, yrkesmässiga och övriga kvalifikationer genomföras.

Utbildningar och övningar avseende cybersäkerhet för egen personal bör vara anpassade utifrån roll, ansvarsområden och befogenheter i arbetet med cybersäkerhet.

Informationsinsatser avseende cybersäkerhet till personal bör inkludera

- grundläggande förståelse för varför cybersäkerhet behövs och hur cybersäkerhet uppnås,
- förståelse för relevanta interna regler och arbetssätt, samt
- vilket stöd som finns tillgängligt för att uppnå cybersäkerhet.

Verksamhetsutövaren bör upprätta en utbildningsplan där det framgår när och hur informationsinsatser, utbildningar och övningar ska genomföras samt när och hur uppföljning och utvärdering ska ske.

Verksamhetsutövaren bör informera personal som avslutar en anställning eller uppdrag om begränsningar i användandet av information som denne har fått tillgång till hos verksamhetsutövaren.

Omvärldsbevakning

10 § För att hålla sig uppdaterad om hot, sårbarheter, teknisk utveckling, rättsliga krav och tillgängligt stöd av betydelse för verksamhetsutövarens cybersäkerhet, ska verksamhetsutövaren bedriva omvärldsbevakning.

Verksamhetsutövaren ska inhämta relevant information från

1. leverantörer av den digitala miljöns hård- och mjukvara, och
2. det nationella cybersäkerhetscentret (NCSC), vid Försvarets radioanstalt, och särskilt de däri ingående funktionerna nationell CSIRT-enhet och cyberkrishanteringsmyndighet.

Allmänna råd

Verksamhetsutövaren bör även som en del av sin omvärldsbevakning inhämta relevant information från

- relevanta tillsynsmyndigheter,
- Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet (NCC-SE) hos det nationella cybersäkerhetscentret (NCSC), samt
- Europeiska unionens cybersäkerhetsbyrå (ENISA).

Informationsklassning

11 § För att identifiera vilka konsekvenser som bristande cybersäkerhet kan få för information som behandlas i system ska verksamhetsutövaren värdera informationen utifrån vilken nivå av skydd informationen behöver ha avseende konfidentialitet, riktighet inklusive autenticitet, och tillgänglighet.

Verksamhetsutövaren ska fastställa antalet nivåer och vilka kriterier som ska användas vid bedömningen av konsekvenser vid informationsklassning.

Allmänna råd

Nivåer och kriterier för informationsklassning bör vara identiska med, eller kunna relateras till, motsvarande nivåer och kriterier för konsekvensbedömning vid riskanalys.

Riskhantering

12 § För att kunna identifiera vilka lämpliga och proportionella säkerhetsåtgärder som ska genomföras ska verksamhetsutövaren identifiera, analysera och värdera risker utifrån deras konsekvens och sannolikhet. Arbetet med risker ska utgå från relevant

1. informationsklassning,
2. information från omvärldsbevakning, samt
3. information om incidenter och tillbud.

Verksamhetsutövaren ska utforma nivåer och tillhörande kriterier för bedömning av konsekvenser och sannolikhet så att risker kan jämföras över tid. Verksamhetsutövaren ska även fastställa kriterier för riskacceptans.

Verksamhetsutövaren ska identifiera och hantera behovet av att uppdatera genomförda riskanalyser vid förändrade hot och nya sårbarheter som kan påverka cybersäkerheten.

Allmänna råd

Risker bör värderas separat för

- informationsbehandling i system,
- förvärv av system,
- utkontrakterad informationsbehandling,
- digitala leveranskedjor,
- mobila system,
- enskilda segment, och
- den digitala miljön i sin helhet.

Verksamhetsutövaren bör omhänderta riskerna med aggregering och ackumulering av information.

13 § För att kunna genomföra lämpliga och proportionella säkerhetsåtgärder ska verksamhetsutövaren vid valet av säkerhetsåtgärder utgå från resultaten av genomförda riskanalyser och fastställda kriterier för riskacceptans.

Valda säkerhetsåtgärder och de risker som dessa säkerhetsåtgärder omhändertar ska dokumenteras i en plan (åtgärdsplan). Av åtgärdsplanen ska det framgå vilken roll eller vilket ansvarsområde som ansvarar för att säkerhetsåtgärden genomförs och när den ska vara genomförd.

Allmänna råd

Åtgärdsplanen bör innehålla en redovisning av vilka andra säkerhetsåtgärder som har övervägts som alternativ för att omhänderta identifierade risker.

Kontinuitetshantering

14 § För att ha beredskap att bedriva verksamhet vid incidenter och kriser med påverkan på cybersäkerheten ska verksamhetsutövaren hantera sitt behov av kontinuitet för sin informationsbehandling och fastställa en prioriteringsordning för återställning av verksamhet. Verksamhetsutövaren ska fastställa och öva alternativa arbetssätt för de verksamheter som bedöms behöva sådana arbetssätt.

Allmänna råd

Verksamhetsutövaren bör fastställa hur och när återgång till ordinarie arbetssätt ska göras efter det att alternativa arbetssätt har använts.

Användning av alternativa arbetssätt samt återställning av sektorskritiska system bör övas vid behov men minst en gång per år.

15 § Verksamhetsutövaren ska för produktionsmiljön

1. fastställa acceptabla tider för otillgänglighet och bristande funktionalitet för informationsbehandling,
2. identifiera och hantera behovet av redundanta funktioner, samt
3. planera för och öva hur situationer med otillgänglighet och bristande funktionalitet ska omhändertas i sektorskritiska system.

För utvecklings-, test-, och utbildningsmiljö ska verksamhetsutövaren identifiera och hantera behovet av att fastställa acceptabla tider för otillgänglighet och bristande funktionalitet, bedöma behovet av redundanta funktioner samt planera för och öva hur situationer med otillgänglighet och bristande funktionalitet ska hanteras.

16 § Verksamhetsutövaren ska identifiera och hantera behovet av att på förhand tydliggöra ytterligare roller, ansvarsområden och befogenheter som krävs för att omhänderta kriser som påverkar verksamhetsutövarens cybersäkerhet (krisorganisation). Verksamhetsutövaren ska identifiera och hantera behovet att på förhand säkerställa tillgång till stöd från relevanta leverantörer.

Incidenthantering

17 § För att minimera konsekvenserna av incidenter och tillbud ska verksamhetsutövaren genom incidenthantering säkerställa att incidenter och tillbud kan identifieras, anmälas, analyseras samt begränsas i omfattning och konsekvens.

Verksamhetsutövaren ska vidta åtgärder för att återställa påverkad information och funktionalitet i system enligt fastställd prioriteringsordning samt förhindra att liknande incidenter sker i den digitala miljön.

Verksamhetsutövaren ska identifiera och hantera behovet av att utreda incidentens grundorsak.

Allmänna råd

Personal och mottagare av externa tjänster bör på ett enkelt sätt kunna anmäla incidenter och tillbud.

Verksamhetsutövaren bör inom incidenthanteringen uppfylla externa krav på rapportering av incidenter och informationsskyldighet till mottagare av externa tjänster som berörs av incidenten.

Vid valet av åtgärder som ska begränsa omfattning och konsekvenser av en incident bör risken för ytterligare incidenter eller tillbud beaktas

Verksamhetsutövaren bör ta stöd från berörda leverantörer vid val av åtgärder för att återställa funktionalitet i system.

Krishantering

18 § För att kunna minimera konsekvenserna av inträffade incidenter som på grund av omfattning eller allvarlighetsgrad inte kan omhändertas inom ordinarie incidenthantering ska verksamhetsutövaren identifiera och hantera behovet av att

1. aktivera sin krisorganisation om sådan finns,
2. vidta åtgärder för att begränsa krisens konsekvenser,
3. säkerställa resurser för att omhänderta uthållighet i verksamheten under krisen, samt
4. genomföra intern och extern kriskommunikation.

Verksamhetsutövaren ska identifiera och hantera behovet av att öva sin krishantering.

Allmänna råd

Vid krishantering bör etablerad stabsmetodik och struktur användas.

Verksamhetsutövaren bör ha tillgång till system för intern och extern kriskommunikation med höga krav på robusthet och tillgänglighet för informationsdelning och samverkan under kriser.

För att stärka förmågan till samverkan och kriskommunikation mellan olika organisationer som kan komma att påverkas vid kriser bör verksamhetsutövaren öva användandet av det webbaserade informationsdelningssystemet WIS som tillhandahålls av Myndigheten för civilt försvar.

Verksamhetsutövaren bör öva sin krishantering avseende sektorsverksamhet vid behov men minst en gång per år.

Uppföljning och utvärdering

19 § För att kunna bedöma effektiviteten av införda säkerhetsåtgärder ska verksamhetsutövaren följa upp och utvärdera om säkerhetsåtgärderna är lämpliga och proportionella i förhållande till externa krav, interna behov och identifierade risker. Verksamhetsutövaren ska även identifiera behov av att förbättra säkerhetsåtgärder.

Uppföljning och utvärdering av säkerhetsåtgärder för sektorskritiska system ska ske vid behov men minst en gång per år.

Allmänna råd

Verksamhetsutövaren bör använda etablerade metoder för uppföljning och utvärdering av säkerhetsåtgärderna såsom granskning, mätning och tester. Dessa kan ske i form av egenkontroll, intern och extern revision.

Uppföljning och utvärdering bör genomföras i samband med

- att säkerhetsåtgärder införs eller förändras,
- förändringar av den digitala miljön som kan påverka cybersäkerheten,
- att förändrade hot eller nya sårbarheter identifieras,
- slutförd grundorsaksanalys, samt
- verksamhetsuppföljning, omorganisation, förändrade rättsliga krav och utkontraktering.

Uppföljning och utvärdering av det systematiska och riskbaserade arbetet med cybersäkerhet bör även omfatta hur fastställda mål och inriktning efterlevs samt hur interna regler, arbetssätt och stöd används och om de motsvarar verksamhetens behov. Vid uppföljning och utvärdering bör även brister och oklarheter avseende tilldelade befogenheter, resurser och arbetsuppgifter samt bristande kompetensförsörjning bedömas.

4 kap. Tekniska och driftrelaterade säkerhetsåtgärder

Förvärv av system och utkontraktering av informationsbehandling

1 § För att säkerställa att verksamhet kan bedrivas med en tillräcklig nivå av cybersäkerhet efter förvärv av system och utkontraktering av informationsbehandling ska verksamhetsutövaren dessförinnan värdera och omhänderta risker som kan uppstå med anledning av detta.

Verksamhetsutövaren ska säkerställa att de krav som ställs på verksamhetsutövaren i denna författning uppfylls av leverantören utom i de delar kravet i sin helhet uppfylls av verksamhetsutövaren.

Verksamhetsutövaren ska utvärdera om den tilltänkta leverantören kan uppfylla ställda krav på cybersäkerhet under hela avtalstiden.

Verksamhetsutövaren ska identifiera och hantera behovet av att, om möjligt, komplettera avtal och överenskommelser som har ingåtts före den 1 oktober 2026 med krav på cybersäkerhet. Risker med avtal och överenskommelser om förvärv och utkontraktering som innehåller otillräckliga krav på cybersäkerhet ska omhändertas.

Allmänna råd

Verksamhetsutövaren bör värdera risker för cybersäkerheten som härrör från eventuella underleverantörer i leveranskedjan.

2 § Verksamhetsutövaren ska identifiera och hantera behovet av kontinuitet i sina digitala leveranskedjor avseende den hård- och mjukvara samt information som behövs för att säkerställa informationsbehandlingen som verksamhetsutövaren behöver för att bedriva intern verksamhet och tillhandahålla externa tjänster.

För att verksamhetsutövaren ska kunna omhänderta svagheter i digitala leveranskedjor, särskilt sådana där alternativa lösningar saknas vid otillgänglig eller otillräcklig leverans, ska verksamhetsutövaren identifiera och hantera behovet av att leverantören ger relevant information om sina underleverantörer.

Allmänna råd

Vid en värdering av risker för de digitala leveranskedjorna bör verksamhetsutövaren beakta resultatet av de samordnade säkerhetsriskbedömningar av kritiska leveranskedjor som utförs i enlighet med artikel 22.1 i NIS 2-direktivet.

Verksamhetsutövaren bör även beakta myndigheters rekommendationer som syftar till att stärka EU:s och Sveriges digitala suveränitet.

3 § Verksamhetsutövaren ska identifiera och hantera behovet av att vid förvärv och utkontraktering välja sådana produkter, tjänster och processer som är certifierade i enlighet med europeiska ordningar för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster enligt artikel 1.1 b i EU:s cybersäkerhetsakt.[2]

[2] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

Allmänna råd

Produkter eller tjänster som ingår i sektorskritiska system bör vara certifierade i enlighet med europeiska ordningar för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster enligt artikel 1.1 b i EU:s cybersäkerhetsakt.

4 § Vid förvärv av system och utkontraktering av informationsbehandling ska verksamhetsutövaren i avtal eller överenskommelse med leverantören säkerställa att lämpliga och proportionella säkerhetsåtgärder kan genomföras och förvaltas över tid.

Allmänna råd

Avtal eller överenskommelse om förvärv av system bör reglera att leverantören kontrollerar hård- och mjukvara i syfte att upptäcka skadlig kod och andra brister i cybersäkerheten innan den levereras till verksamhetsutövaren.

Innan avtal eller överenskommelser tecknas om utkontraktering av informationsbehandling bör verksamhetsutövaren kontrollera att informationsklassning är genomförd för den information som ska utkontrakteras och riskerna med utkontrakteringen är omhändertagna.

Avtal eller överenskommelse om utkontraktering av informationsbehandling bör reglera vilka säkerhetsåtgärder leverantören ska vidta inklusive

- att verksamhetsutövaren får kontaktuppgifter till hos leverantören utsedd systemägare,
- vilken kompetens avseende cybersäkerhet leverantören behöver ha,
- när och hur leverantören ska informera verksamhetsutövaren, om misstänkta och inträffade incidenter och tillbud, om identifierade hot och sårbarheter samt om förändringar i system som kan påverka efterlevnaden av ställda krav på säkerhetsåtgärder,
- hur risker i verksamhetsutövarens digitala leveranskedjor som härrör från leverantörens underleverantörer ska omhändertas och delges verksamhetsutövaren,
- att leverantören kontrollerar hård- och mjukvara i syfte att upptäcka skadlig kod och andra brister i cybersäkerheten innan den används för verksamhetsutövarens informationsbehandling,
- i vilken omfattning leverantören ska öva incident-, kontinuitets- och krishantering med verksamhetsutövaren,
- hur leverantören ska följa upp sin egen och eventuella underleverantörers efterlevnad av ställda krav på säkerhetsåtgärder,
- hur verksamhetsutövaren ska följa upp leverantörens efterlevnad av ställda krav på säkerhetsåtgärder,
- att avtalsförhållandet ska kunna sägas upp i förtid om leverantören brister i efterlevnad av ställda krav på säkerhetsåtgärder, samt
- hur verksamhetsutövarens information ska återlämnas eller förstöras när avtalet upphör.

Innan utkontrakterad informationsbehandling inleds bör verksamhetsutövaren kontrollera att riskerna med utkontrakteringen är omhändertagna, informationsägare är utsedda för den informationshantering som utkontrakteras, och tilltänkt leverantör uppfyller ställda krav på säkerhetsåtgärder.

Utveckling, underhåll och avveckling av system

5 § För att motverka att sårbarheter uppstår vid utveckling och underhåll av den digitala miljön ska verksamhetsutövaren inför och under utvecklingen samt vid underhåll av system säkerställa att

1. informationsägare och systemägare involveras i arbetet med att identifiera behov av och att införa säkerhetsåtgärder,
2. informationsklassning har genomförts och hålls uppdaterad,
3. riskanalys är genomförd och hålls uppdaterad,
4. åtgärdsplanen hålls uppdaterad, och
5. etablerade metoder för säker utveckling följs.

6 § Innan beslut fattas om att för första gången driftsätta ett system i den digitala miljön ska verksamhetsutövaren säkerställa att

1. det finns nödvändig dokumentation för drift och förvaltning,
2. säkerhetstester och granskningar har genomförts för att säkerställa att införda tekniska och driftrelaterade säkerhetsåtgärder är lämpliga och proportionella,
3. tilldelade resurser för drift och underhåll av systemet är tillräckliga,
4. identifierade behov av säkerhetsåtgärder för systemet är omhändertagna, och
5. beslut om att påbörja informationsbehandlingen i systemet har fattats.

Framkommer brister avseende första stycket p. 1–5 ska dessa dokumenteras och eventuella risker med bristerna omhändertas.

Om utveckling och underhåll av redan driftsatt system kan påverka cybersäkerheten i den digitala miljön ska verksamhetsutövaren säkerställa att p. 1–5 omhändertas.

7 § För att upprätthålla skyddet för information under avveckling av system ska verksamhetsutövaren, innan avvecklingen påbörjas, säkerställa att

1. tilldelade resurser för avveckling av systemet är tillräckliga,
2. beslut om att avveckla informationsbehandlingen har fattats,
3. risker med avvecklingen har omhändertagits, och
4. åtgärdsplan för avvecklingen finns.

Driftrelaterad dokumentation

8 § För att kunna upprätthålla säker drift ska verksamhetsutövaren hålla dokumentation över arkitekturen för den digitala miljön uppdaterad.

Allmänna råd

Av dokumentationen för den digitala miljön bör framgå

- vilka miljöer den är indelad i, det vill säga produktions-, utvecklings-, test- och utbildningsmiljö,

- vad respektive miljö innehåller avseende segment, system, hårdvara, och mjukvara,
- vilka informationsflöden som finns mellan olika miljöer, mellan system, samt till och från den digitala miljön, och hur kritiska informationsflödena är för verksamheten, samt
- vilken verksamhet, om någon, som bedrivs med stöd av utkontrakterad informationsbehandling.

Tekniskt systemstöd bör användas för att hålla dokumentationen uppdaterad. Arkitekturen bör visualiseras i en systemkarta.

---

9 § För att verksamhetsutövaren skyndsamt ska kunna omhänderta sårbarheter och incidenter i den digitala miljön samt bedöma konsekvenserna av dessa ska verksamhetsutövaren hålla en uppdaterad förteckning över relevant information om den digitala miljön.

Allmänna råd

Förteckningen över den digitala miljön bör innehålla information om

- vilka system som ingår i produktionsmiljön samt kontaktuppgifter till berörda systemägare och informationsägare,
- kontaktuppgifter till leverantörer av hård- och mjukvara som används i produktionsmiljön,
- vilka system som är sektorskritiska och vilka som används för att tillhandahålla verksamhetsutövarens externa tjänster, samt
- vilka, om några, system i utvecklings-, test- eller utbildningsmiljö som bedöms vara kritiska för att skyndsamt kunna omhänderta sårbarheter och incidenter i produktionsmiljön.

Verksamhetsutövaren bör dokumentera vilken informationsbehandling som är utkontrakterad samt kontaktuppgifter till leverantören och till verksamhetsutövarens berörda informationsägare. Förteckningen bör även innehålla kontaktuppgifter till sådana funktioner hos leverantörer som ger stöd vid sårbarheter och incidenter.

---

10 § För att kunna upprätthålla säker drift och möjliggöra återställning av system i produktionsmiljön ska verksamhetsutövaren hålla driftdokumentationen för systemen uppdaterad samt fastställa vilka system som är sektorskritiska.

För utvecklings-, test- och utbildningsmiljö ska verksamhetsutövaren identifiera och hantera behovet av att hålla driftdokumentation för system uppdaterad.

Allmänna råd

Av driftdokumentationen för ett system bör framgå

- vilken verksamhet och vilken informationsbehandling som systemet stödjer samt om systemet används för sektorskritisk verksamhet,
- om och varför systemet är nödvändigt för att upprätthålla viktiga samhällsfunktioner hos andra organisationer,
- om information i behov av utökat skydd behandlas i systemet,
- referens till aktuell riskanalys och risker som inte kunnat omhändertas på ett tillfredställande sätt,
- vilken nivå av cybersäkerhet som systemet behöver uppnå och vilka säkerhetsåtgärder som har genomförts för att uppnå denna,
- beroenden till andra system,
- acceptabla tider för otillgänglighet och bristande funktionalitet och hur systemet återställs,
- om systemet är placerat i it-segment eller ot-segment,
- vilken hårdvara som används och dess version samt vilken mac-adress, ip-adress eller identifierare som används för hårdvara,
- vilken mjukvara som används och dess version,
- hur hård- och mjukvara är konfigurerad,
- resurser som behövs för drift och underhåll av systemet,
- kontaktuppgifter till berörd systemägare och till berörda informations-ägare, samt
- referens till relevanta användarmanualer för systemet.

Segmentering

11 § För att minimera konsekvenser och förhindra spridning av incidenter orsakade av angrepp mot och misstag i den digitala miljön ska verksamhets-utövaren dela in den i segment och endast tillåta godkända informations-flöden till och från segment.

Verksamhetsutövaren ska identifiera och hantera behovet av att placera enskilda system, ett begränsat antal system eller system med liknande funktion, användning eller skyddsbehov i olika it- eller ot-segment i den digitala miljön.

Allmänna råd

Verksamhetsutövaren bör införa segment i produktionsmiljön för

- system som används för gästnätverk,
- system hos verksamhetsutövaren som sammankopplas med system hos leverantör,
- system som tillhandahåller externa tjänster,
- system som innehåller sårbarheter som inte kan omhändertas på ett tillfredställande sätt,

- klienter för användare,
- klienter för systemadministration,
- sektorskritiska system,
- centrala säkerhetsfunktioner i form av behörighetshantering säkerhetsloggning, säkerhetskopiering, övervakning av system, filtrering av extern kommunikation och liknande,
- centrala stödfunktioner i form av skrivare, skanner och liknande funktioner, samt
- trådlösa nätverk för personal.

---

12 § Verksamhetsutövaren ska bedriva utveckling, test och utbildning som kan påverka säkerheten i produktionsmiljöns it-segment i en från produktionsmiljön avskild utvecklings-, test- respektive utbildningsmiljö.

Verksamhetsutövaren ska identifiera och hantera behovet av att bedriva utveckling, test och utbildning som kan påverka säkerheten i produktionsmiljöns ot-segment i en från produktionsmiljön avskild utvecklings-, test- respektive utbildningsmiljö.

Säkerhetskonfigurering

13 § För att försvåra angrepp mot system ska de konfigureras så att obehörig åtkomst försvåras och cybersäkerheten upprätthålls.

Verksamhetsutövaren ska

1. byta ut förinställda autentiseringsuppgifter och stänga av, blockera eller ta bort funktioner i system som inte behövs,
2. endast tillåta godkända informationsflöden till och från system, samt
3. identifiera och hantera behovet av att endast tillåta installation och användning av på förhand godkänd mjukvara.

Allmänna råd

Verksamhetsutövaren bör inte tillåta direktkommunikation mellan klienter. Inaktiva sessioner bör automatiskt avslutas efter en fördefinierad tidsperiod.

Vid säkerhetskonfigurering bör leverantörens rekommendationer och relevanta standarder användas och säkerhetsfunktioner bör konfigureras så att säkerhet upprätthålls när tekniska fel och brister inträffar.

Behörighetshantering och autentisering

14 § För att säkerställa att endast behöriga användare och system ska få åtkomst till olika delar av den digitala miljön ska verksamhetsutövaren genom behörighetshantering fastställa hur digitala identiteter, behörigheter och autentiseringsuppgifter utformas, tilldelas, används, förändras, avslutas och skyddas.

Verksamhetsutövaren ska säkerställa att autentiseringsuppgifter har tillräcklig längd och komplexitet.

Allmänna råd

Verksamhetsutövaren bör

- tidsbegränsa tilldelade digitala identiteter och behörigheter,
- använda tekniska system som stöd för hantering och kontroll av digitala identiteter, behörigheter och autentiseringsuppgifter, samt
- identifiera vilka externa tjänster som ska vara åtkomliga utan kontroll av digitala identiteter eller behörigheter.

15 § Verksamhetsutövaren ska låsa en digital identitet efter ett fastställt antal misslyckade inloggningsförsök.

Verksamhetsutövaren ska låsa, blockera eller ta bort digitala identiteter för användare eller system som inte längre ska ha åtkomst till system eller den digitala miljön.

16 § Verksamhetsutövaren ska inte tilldela användare och system behörighet till mer information eller fler system än vad som behövs för att bedriva verksamheten och upprätthålla cybersäkerheten.

Systemadministrativ behörighet ska tilldelas restriktivt och endast användas för systemadministration.

Verksamhetsutövaren ska inte tillåta att autentiseringsuppgifter som används i produktionsmiljön också används i utvecklings-, test- och utbildningsmiljö.

Allmänna råd

Verksamhetsutövaren bör

- genomföra åtkomstkontroll till information i centrala stödfunktioner i form av skrivare, skanner och liknande utrustning innan åtkomst beviljas,
- administrera olika segment av produktionsmiljön med olika systemadministrativa behörigheter, samt
- begränsa omfattning och tid för systemadministrativa behörigheter som ges till leverantörer till aktuellt uppdrag.

17 § Verksamhetsutövaren ska använda flerfaktorsautentisering för åtkomst till system i it-segment som behandlar information som har behov av utökat skydd. Verksamhetsutövaren ska använda flerfaktorsautentisering för systemadministrativ åtkomst till system i it-segment och till ot-segment i produktionsmiljön. Flerfaktorsautentisering ska även användas för personals och leverantörers åtkomst till den digitala miljön via externt nätverk.

Verksamhetsutövaren ska identifiera och hantera behov av flerfaktorsautentisering vid annan åtkomst till information och system i den digitala miljön.

18 § Verksamhetsutövaren ska identifiera och hantera behovet av att mottagare av externa tjänster identifierar sig med e-legitimation eller motsvarande för att få åtkomst till sådana tjänster.

19 § Verksamhetsutövaren ska identifiera och hantera behovet av att andra organisationer och enskilda personer kan verifiera verksamhetsutövarens identitet vid kontakt via digitala kanaler.

Allmänna råd

Andra organisationer och enskilda personer bör kunna verifiera verksamhetsutövarens identitet vid dennes kommunikation via e-post, sms, telefonsamtal och webbsidor. Verksamhetsutövaren bör tillhandahålla lättillgänglig information om hur sådan verifiering kan ske.

Övervakning, säkerhetsloggning och logganalys

20 § För att upptäcka och agera på tekniska fel, intrång och andra brister i cybersäkerheten ska verksamhetsutövaren identifiera och hantera behovet av att övervaka den digitala miljön. Verksamhetsutövaren ska även identifiera och hantera behovet av att larm genereras vid brister i cybersäkerheten och att åtgärder vidtas vid sådana larm.

Verksamhetsutövaren ska, om inte uppenbart obehövligt, ansluta sig till automatiska notifieringar av tekniska sårbarheter (ANTS) hos den nationella CSIRT-enheten.

Verksamhetsutövaren ska identifiera och hantera behovet av att, om möjligt, ansluta sig till stöd för informationsutbyte om cyberhot (MISP-SE) hos den nationella CSIRT-enheten.

Verksamhetsutövaren ska identifiera och hantera behovet av realtids-övervakning i den digitala miljön.

Allmänna råd

Verksamhetsutövaren bör använda realtidsövervakning i produktionsmiljön för att skyndsamt upptäcka och agera på incidenter och tillbud i centrala säkerhets-funktioner och sektorskritiska system.

21 § För att kunna utreda brister i cybersäkerheten ska verksamhetsutövaren logga relevanta säkerhetshändelser. Verksamhetsutövaren ska logga obehörig åtkomst och försök till obehörig åtkomst till den digitala miljön.

Verksamhetsutövarens säkerhetsloggning ska även, om det inte är uppenbart obehövligt, omfatta följande i produktionsmiljön

1. åtkomst till system och segment,
2. användning av systemadministrativ behörighet,
3. förändring av konfigurationer i centrala säkerhetsfunktioner och sektorskritiska system,
4. förändring av behörighet för användare och system, och
5. åtkomst till information i behov av utökat skydd.

Verksamhetsutövaren ska identifiera och hantera behovet av säkerhetsloggning i utvecklings-, test- och utbildningsmiljö.

Säkerhetsloggarna ska skyddas mot obehörig åtkomst och sparas så länge de behövs för att kunna utreda brister i cybersäkerheten.

Allmänna råd

För att möjliggöra utredning av fel, intrång och andra brister i cybersäkerheten bör säkerhetsloggar innehålla tillräcklig information om vilken händelse som har inträffat, vilken användare och vilket system som registrerade säkerhetshändelsen först, vilken information och vilka system som har påverkats samt vid vilken tidpunkt som händelsen inträffade.

Verksamhetsutövaren bör logga åtkomst till produktionsmiljön och till system som förutsätter en tilldelad behörighet.

Verksamhetsutövaren bör logga obehörig åtkomst och försök till obehörig åtkomst i utvecklings-, test- och utbildningsmiljö.

Verksamhetsutövaren bör logga samtliga händelser som indikerar brister i cybersäkerheten och som upptäckts genom övervakning.

22 § Verksamhetsutövaren ska analysera säkerhetsloggarna för att upptäcka och utreda fel, obehörig åtkomst och andra brister i cybersäkerheten.

Verksamhetsutövaren ska analysera säkerhetsloggar för varje system med ett intervall som är lämpligt utifrån externa krav, interna behov och identifierade risker.

Allmänna råd

Verksamhetsutövaren bör använda ett centralt systemstöd för att samla in, lagra och analysera säkerhetsloggarna.

Robust och korrekt tid

23 § För att kunna jämföra säkerhetsloggar vid incidenter som involverar andra organisationer ska verksamhetsutövaren använda robust och korrekt tid som är översättningsbar till den svenska tillämpningen av koordinerad universell tid, UTC (SP), i produktionsmiljön.

För utvecklings-, test- och utbildningsmiljö ska verksamhetsutövaren identifiera och hantera behovet av att använda robust och korrekt tid som är översättningsbar till den svenska tillämpningen av koordinerad universell tid, UTC (SP).

Allmänna råd

Verksamhetsutövaren bör använda tidstjänsten Swedish Distributed Time Service för robust och korrekt tid koordinerad till UTC (SP) som tillhandahålls på uppdrag av behörig myndighet.

Skydd mot skadlig kod

24 § För att skydda system i it-segment mot angrepp med skadlig kod ska verksamhetsutövaren använda för detta ändamål avsedd mjukvara om sådan mjukvara uppfyller verksamhetsutövarens behov och finns tillgänglig på marknaden.

Allmänna råd

Verksamhetsutövaren bör skydda system i ot-segment mot angrepp med skadlig kod genom att använda för detta ändamål avsedd mjukvara om sådan mjukvara uppfyller verksamhetsutövarens behov och finns tillgänglig på marknaden.

Kryptering

25 § För att säkerställa att information i system skyddas mot obehörig åtkomst och obehörig förändring vid överföring mellan och lagring i system ska verksamhetsutövaren identifiera och hantera behovet av att kryptera informationen i den digitala miljön.

Verksamhetsutövaren ska använda kryptering för att skydda säkerhetsloggar och autentiseringsuppgifter vid överföring i den digitala miljön. Säkerhetsloggar, autentiseringsuppgifter och annan information i behov av utökat skydd ska skyddas med kryptering vid överföring till system utanför den digitala miljön.

Allmänna råd

Verksamhetsutövaren bör fastställa kriterier för val och godkännande av krypteringsalgoritmer, krypteringsprotokoll och nyckellängder samt fastställa när och hur krypteringsnycklar genereras, distribueras, används, återkallas, skyddas och förstörs.

Verksamhetsutövaren bör skydda säkerhetsloggar, autentiseringsuppgifter och information i behov av utökat skydd med kryptering vid lagring i den digitala miljön.

26 § För att försvåra angrepp genom manipulation av översättningen mellan domännamn och ip-adresser i domännamnssystemet (DNS) ska verksamhetsutövaren, om inte uppenbart obehövligt, använda Domain Name System Security Extensions (DNSSEC) för domännamn som verksamhetsutövaren registrerat i DNS.

Säkerhetstester och granskningar

27 § För att identifiera bristande cybersäkerhet för system i it-segment ska verksamhetsutövaren genom säkerhetstester och granskningar säkerställa att införda tekniska och driftrelaterade säkerhetsåtgärder är lämpliga och proportionella. Säkerhetstester ska användas för att kontrollera att

1. systemen är uppdaterade till senaste godkända version,
2. publicerade sårbarheter är omhändertagna, och
3. valda konfigurationer har införts.

Granskningar ska användas för att kontrollera att införda tekniska och driftrelaterade säkerhetsåtgärder omhändertar systemets behov av cybersäkerhet.

Verksamhetsutövaren ska identifiera och hantera behovet av att genom säkerhetstester och granskningar säkerställa att införda tekniska och drift-relaterade säkerhetsåtgärder för system i ot-segment är lämpliga och proportionella.

Allmänna råd

Etablerad testmetodik bör användas för både automatiserade och manuella säkerhetstester.

Om sårbarheter som inte tidigare har publicerats upptäcks bör dessa rapporteras till den nationella CSIRT-enheten.

Återställning av förlorad information och säkerhetskopiering

28 § För att minska konsekvenserna för verksamheten om informationen i system har förlorats, förvanskats eller på annat sätt blivit otillgänglig, ska verksamhetsutövaren säkerställa att informationen kan återställas inom fastställda acceptabla tider för otillgänglighet och bristande funktionalitet.

Verksamhetsutövaren ska identifiera och hantera behovet av att säkerhetskopiera informationen.

Allmänna råd

För säkerhetskopiering bör det fastställas

- vilken information som ska säkerhetskopieras avseende programvara, konfiguration respektive behandlad information,
- hur ofta och på vilket sätt säkerhetskopior ska tas och hur kontroll ska göras av att informationen på säkerhetskopiorna är korrekt och komplett,
- hur säkerhetskopior ska skyddas mot obehörig åtkomst, obehörig förändring och fysisk skada och var och hur länge säkerhetskopiorna ska sparas, samt,
- hur återläsning av säkerhetskopior ska genomföras, och hur kontroll ska göras av att informationen som återlästs är korrekt och komplett

Minst en säkerhetskopia bör skyddas mot skadlig kod genom att lagras på hårdvara separerad från det system som informationen hämtats ifrån.

Intrångsdetektering och intrångsskydd

29 § För att upptäcka och förhindra angrepp ska verksamhetsutövaren använda intrångsdetektering och intrångsskydd för it-segment i produktionsmiljön.

Verksamhetsutövaren ska identifiera och hantera behovet av intrångsdetektering och intrångsskydd för ot-segment i produktionsmiljön.

För utvecklings-, test- och utbildningsmiljö ska verksamhetsutövaren identifiera och hantera behovet av intrångsdetektering och intrångsskydd.

Ändringshantering

30 § För att minska risken för incidenter och tillbud som kan uppkomma vid ändringar ska verksamhetsutövaren bedriva ändringshantering för produktionsmiljön på ett strukturerat och spårbart sätt vid införande, uppgradering, uppdatering och avveckling av hård- och mjukvara samt andra förändringar som påverkar cybersäkerheten.

För utvecklings-, test- och utbildningsmiljö ska verksamhetsutövaren identifiera och hantera behovet av att bedriva ändringshantering på ett strukturerat och spårbart sätt.

Allmänna råd

Endast ändringar som godkänts genom ändringshanteringen bör genomföras. Mjukvara bör uppdateras till senaste version utan onödigt dröjsmål.

Verksamhetsutövaren bör fastställa vilka åtgärder som ska vidtas när en uppdatering eller uppgradering inte kan genomföras eller när pågående ändring behöver avbrytas.

31 § För att skydda system i it-segment mot sårbarheter ska verksamhetsutövaren skyndsamt genomföra säkerhetsuppdateringar. Mjukvara som leverantören inte längre tillhandahåller säkerhets-uppdateringar för ska bytas ut eller uppgraderas utan onödigt dröjsmål.

Verksamhetsutövaren ska identifiera och hantera behovet av säkerhetsuppdateringar, uppdateringar och uppgraderingar i ot-segment.

Allmänna råd

Verksamhetsutövaren bör påbörja arbetet med att införa en säkerhetsuppdatering inom 72 timmar efter det att programvara som ger skydd mot sårbarheten har tillgängliggjorts.

5 kap. Fysiska säkerhetsåtgärder

Lokaler

1 § För att förhindra obehörig fysisk åtkomst till, förlust av och fysisk skada på system ska verksamhetsutövaren skydda verksamhetens lokaler där information behandlas i system mot obehörigt tillträde genom tillträdesbegränsning och, om inte uppenbart obehövligt, bevakning.

Verksamhetsutövaren ska kontrollera personals samt besökares identitet innan de ges tillträde till sådana lokaler förutom till utpekade besöksutrymmen.

Verksamhetsutövaren ska identifiera och hantera behovet av särskilda it- och ot-utrymmen samt behovet av annat fysiskt skydd för utrustning.

Allmänna råd

Verksamhetsutövaren bör anpassa skalskydd för verksamhetens lokaler utifrån den information som behandlas där.

Verksamhetsutövaren bör i verksamhetens lokaler behandla information i behov av utökat skydd i sektioner skilda ifrån övriga lokaler.

Verksamhetsutövaren bör placera servrar och nätverksutrustning i särskilda it- och ot-utrymmen, tilldela tillträde till sådana utrymmen restriktivt och registrera tillträde på individnivå.

2 § Verksamhetsutövaren ska säkerställa, om det inte är uppenbart obehövligt, att särskilda it- och ot-utrymmen förses med bevakning och larm samt att åtgärder vidtas vid larm om obehörigt tillträde.

Verksamhetsutövaren ska identifiera och hantera behovet av att larm genereras vid obehörigt tillträde till verksamhetens övriga lokaler och att åtgärder vidtas vid sådana larm.

3 § För att undvika förlust av, skada på eller funktionsstörning i system ska verksamhetsutövaren identifiera och hantera behovet av att skydda lokaler mot

1. brand,
2. vattenskador,
3. skadlig nivå av luftfuktighet, och
4. skadlig temperatur.

Tekniska försörjningssystem

4 § För att undvika skada på eller störning i system i den digitala miljön på grund av fel eller avbrott i tekniska försörjningssystem ska verksamhetsutövaren säkerställa tillräcklig funktionalitet avseende el, kyla, värme och ventilation samt externa elektroniska kommunikationsnät och externa elektroniska kommunikationstjänster.

Verksamhetsutövaren ska identifiera och hantera behovet av att övervaka de tekniska försörjningssystemens funktion, att larm genereras vid otillräcklig funktionalitet samt att åtgärder vidtas vid sådana larm.

Verksamhetsutövaren ska identifiera och hantera behovet av redundanta funktioner för tekniska försörjningssystem.

6 kap. Sektorsspecifika säkerhetsåtgärder

Offentlig förvaltning

System för kriskommunikation

1 § För att kunna samverka och kommunicera vid kriser ska verksamhetsutövare kontrollera cybersäkerheten i system som ska användas för samverkan respektive intern och extern kriskommunikation.

Allmänna råd

Verksamhetsutövaren bör kontrollera att system för samverkan respektive kriskommunikation kan användas på avsett sätt var tredje månad.

2 § Verksamhetsutövare ska identifiera och hantera behovet av att, om möjligt, använda Rakelterminaler (Radiokommunikation för effektiv ledning) eller SWEN-terminaler (The Swedish Emergency Network) och SGSI (Swedish Government Secure Intranet) för kriskommunikation.

7 kap. Undantag

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

Denna författning träder i kraft den 1 oktober 2026.

Myndigheten för civilt försvar

MIKAEL FRISELL

Tove Wätterstam
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: 19126-11