NATIONELLT CYBERSÄKERHETSCENTER
En del av FRA

Föreskriftsvägledning - föreskrifterna om säkerhetsåtgärder och ledningens utbildning

Cybersäkerhetslagen

Ärendenummer: 2026FRA1970

Föreskriftsvägledning till föreskrifterna om säkerhetsåtgärder och ledningens utbildning

Det här är en föreskriftsvägledning som är tänkt som stöd för verksamhetsutövare som omfattas av cybersäkerhetslagens regler vid tillämpning av föreskrifterna om säkerhetsåtgärder och ledningens utbildning (MCFFS 2026:11) för väsentliga och viktiga verksamhetsutövare. Vägledningen riktar sig både till verksamhetsutövare och tillsynsmyndigheter.

Föreskriftsvägledningen tillhandahåller endast information som stöd för tolkningen av regleringen, den inför inte några nya krav. Förtydliganden och förklaringar i denna vägledning ska inte betraktas som förhandsbesked om vad tillsynsmyndigheterna kan komma att bedöma i ett enskilt tillsynsärende.

Ort, Ange datum.

John Billow
chef Nationellt Cybersäkerhetscenter - NCSC

Nationellt cybersäkerhetscenter (NCSC)
Försvarets radioanstalt, Box 301, 161 26 Bromma
E-post: ncsc@ncsc.se Webbplats: www.ncsc.se Telefon: 010-382 80 00

Innehållsförteckning

Innehållsförteckning **2**
1 Inledning **1**
2 Innebörden av föreskrifter och allmänna råd **2**
3 Tillsyn **2**
4 Föreskrifternas utformning **2**
4.1 Föreskrifternas disposition 3
4.2 Närmare om utformning av kraven 4
5 Uttryck och tidsangivelser **5**
5.1 Beskrivning av hur krav ska omhändertas 5
5.2 Tidsfrister 6
5.3 Grundläggande begrepp 7
6 Andra kapitlet Ledningens utbildning **17**
6.1 Ledningens utbildning 2 kap. 1 § 17
6.1.1 Introduktion 17
6.1.2 Krav 17
6.1.3 Tolkningsstöd 18
6.1.4 Kopplingar till andra paragrafer 19
7 Tredje kapitlet Organisatoriska säkerhetsåtgärder **20**
7.1 Systematiskt och riskbaserat arbete med cybersäkerhet 1–2 §§ 20
7.1.1 Introduktion 20
7.1.2 Krav 20
7.1.3 Tolkningsstöd 21
7.1.4 Kopplingar till andra paragrafer 22
7.2 Interna regler och arbetssätt 3 kap. 3 § 22
7.2.1 Introduktion 22
7.2.2 Krav 23
7.2.3 Tolkningsstöd 24
7.2.4 Kopplingar till andra paragrafer 24
7.3 Roller, ansvarsområden och befogenheter 3 kap. 4–8 §§ 25

7.3.1 Introduktion 25
7.3.2 Krav 25
7.3.3 Tolkningsstöd 27
7.3.4 Kopplingar till andra paragrafer 30
Personalsäkerhet 3 kap. 9 § 30
7.3.5 Introduktion 30
7.3.6 Krav 31
7.3.7 Tolkningsstöd 31
7.3.8 Kopplingar till andra paragrafer 32
Omvärldsbevakning 3 kap. 10 § 32
7.3.9 Introduktion 32
7.3.10 Krav 33
7.3.11 Tolkningsstöd 33
7.3.12 Kopplingar till andra paragrafer 34
7.4 Informationsklassning 3 kap. 11 § 34
7.4.1 Introduktion 34
7.4.2 Krav 34
7.4.3 Tolkningsstöd 34
7.4.4 Kopplingar till andra paragrafer 35
7.5 Riskhantering 3 kap. 12–13 §§ 35
7.5.1 Introduktion 35
7.5.2 Krav 36
7.5.3 Tolkningsstöd 37
7.5.4 Kopplingar till andra paragrafer 38
7.6 Kontinuitetshantering 3 kap. 14–16 §§ 39
7.6.1 Introduktion 39
7.6.2 Krav 39
7.6.3 Tolkningsstöd 40
7.6.4 Kopplingar till andra paragrafer 41
7.7 Incidenthantering 3 kap. 17 § 41
7.7.1 Introduktion 41
7.7.2 Krav 42
7.7.3 Tolkningsstöd 42

7.7.4 Kopplingar till andra paragrafer 43
7.8 Krishantering 3 kap. 18 § 43
7.8.1 Introduktion 43
7.8.2 Krav 44
7.8.3 Tolkningsstöd 44
7.8.4 Kopplingar till andra paragrafer 45
7.9 Uppföljning och utvärdering 3 kap. 19 § 46
7.9.1 Introduktion 46
7.9.2 Krav 46
7.9.3 Tolkningsstöd 47
7.9.4 Kopplingar till andra paragrafer 47
8 Fjärde kapitlet Tekniska och driftrelaterade säkerhetsåtgärder 47
8.1 Förvärv av system och utkontraktering av informationsbehandling 4 kap. 1 – 4 §§ 47
8.1.1 Introduktion 47
8.1.2 Krav 48
8.1.3 Tolkningsstöd 50
8.1.4 Kopplingar till andra paragrafer 52
8.2 Utveckling, underhåll och avveckling av system 4 kap. 5 – 7 §§ 52
8.2.1 Introduktion 52
8.2.2 Krav 53
8.2.3 Tolkningsstöd 54
8.2.4 Kopplingar till andra paragrafer 54
8.3 Driftrelaterad dokumentation 4 kap. 8–10 §§ 54
8.3.1 Introduktion 54
8.3.2 Krav 55
8.3.3 Tolkningsstöd 56
8.3.4 Kopplingar till andra paragrafer 57
8.4 Segmentering 11–12 §§ 57
8.4.1 Introduktion 57
8.4.2 Krav 57
8.4.3 Tolkningsstöd 58
8.4.4 Kopplingar till andra paragrafer 60

8.5 Säkerhetskonfigurering 4 kap. 13 § 60
8.5.1 Introduktion 60
8.5.2 Krav 60
8.5.3 Tolkningsstöd 61
8.5.4 Kopplingar till andra paragrafer 62
8.6 Behörighetshantering och autentisering 4 kap. 14 – 19 §§ 62
8.6.1 Introduktion 62
8.6.2 Krav 63
8.6.3 Tolkningsstöd 65
8.6.4 Kopplingar till andra paragrafer 66
8.7 Övervakning, säkerhetsloggning och logganalys 4 kap. 20 – 22 §§ . 66
8.7.1 Introduktion 66
8.7.2 Krav 66
8.7.3 Tolkningsstöd 68
8.7.4 Kopplingar till andra paragrafer 69
8.8 Robust och korrekt tid 4 kap. 23 § 69
8.8.1 Introduktion 69
8.8.2 Krav 69
8.8.3 Tolkningsstöd 69
8.8.4 Kopplingar till andra paragrafer 70
8.9 Skydd mot skadlig kod 4 kap. 24 § 70
8.9.1 Introduktion 70
8.9.2 Krav 70
8.9.3 Tolkningsstöd 71
8.9.4 Kopplingar till andra paragrafer 71
8.10 Kryptering 4 kap. 25–26 §§ 71
8.10.1 Introduktion 71
8.10.2 Krav 71
8.10.3 Tolkningsstöd 72
8.10.4 Kopplingar till andra paragrafer 73
8.11 Säkerhetstester och granskningar 4 kap. 27 § 73
8.11.1 Introduktion 73
8.11.2 Krav 73

8.11.3 Tolkningsstöd 74
8.11.4 Kopplingar till andra paragrafer 75
8.12 Återställning av förlorad information och säkerhetskopiering 4 kap. 28 § 75
8.12.1 Introduktion 75
8.12.2 Krav 76
8.12.3 Tolkningsstöd 76
8.12.4 Kopplingar till andra paragrafer 77
8.13 Intrångsdetektering och intrångsskydd 4 kap. 29 § 77
8.13.1 Introduktion 77
8.13.2 Krav 77
8.13.3 Tolkningsstöd 77
8.13.4 Kopplingar till andra paragrafer 78
8.14 Ändringshantering 4 kap. 30 – 31 §§ 78
8.14.1 Introduktion 78
8.14.2 Krav 78
8.14.3 Tolkningsstöd 79
8.14.4 Kopplingar till andra paragrafer 80
9 Femte kapitlet Fysiska säkerhetsåtgärder 80
9.1 Lokaler 5 kap. 1–3 §§ 80
9.1.1 Introduktion 80
9.1.2 Krav 80
9.1.3 Tolkningsstöd 81
9.1.4 Kopplingar till andra paragrafer 82
9.2 Tekniska försörjningssystem 5 kap. 4 § 82
9.2.1 Introduktion 82
9.2.2 Krav 83
9.2.3 Tolkningsstöd 83
9.2.4 Kopplingar till andra paragrafer 84
10 Sjätte kapitlet Sektorsspecifika säkerhetsåtgärder 84
10.1 Offentlig förvaltning 84
10.2 System för kriskommunikation 6 kap. 1–2 §§ 84
10.2.1 Introduktion 84

10.2.2 Krav 84
10.2.3 Tolkningsstöd 85
10.2.4 Kopplingar till andra paragrafer 85
11 Sjunde kapitlet Undantag 86
11.1.1 Krav 86
11.1.2 Tolkningsstöd 86

1 Inledning

Cybersäkerhetslagen (2025:1506), hädanefter kallad CSL, med tillhörande föreskrifter och allmänna råd syftar till att höja den generella cybersäkerhetsnivån i Sverige inom 18 utpekade sektorer som bedöms vara viktiga för samhällets funktion och ekonomi. För att nå dit ställer CSL bland annat krav på de som omfattas av lagen att vidta säkerhetsåtgärder.

Den 1 oktober 2026 träder föreskrifter och allmänna råd om säkerhetsåtgärder och ledningens utbildning för väsentliga och viktiga verksamhetsutövare (MCFFS 2026:11) i kraft. Dessa förtydligar och kompletterar CSL:s bestämmelser om säkerhetsåtgärder och utbildning. CSL ställer bland annat krav på att en verksamhetsutövare ska vidta lämpliga och proportionella åtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter (2 kap. 3 § CSL) samt att de som ingår i ledningen för en verksamhetsutövare ska genomgå utbildning om säkerhetsåtgärder (2 kap. 4 § CSL).

Den 1 juli 2026 övergick föreskriftsrätten enligt cybersäkerhetsförordningen (2025:1507) från Myndigheten för civilt försvar (MCF) till Försvarets Radioanstalt (FRA). Det innebär att FRA tar över ansvaret för MCF:s föreskrifter enligt CSL och framtida revideringar. Föreskrifterna gäller oförändrat och bär MCF:s namn tills att de har reviderats.

2 Innebörden av föreskrifter och allmänna råd

Föreskrifter (”ska-krav”) kompletterar och förtydligar bestämmelser i lag. De aktörer som träffas av bestämmelserna är skyldiga att efterleva såväl krav som finns i lag som i tillhörande föreskrifter.

Allmänna råd (”bör-krav”) innehåller förtydliganden och konkreta förslag på tillvägagångsätt för att uppfylla föreskrifternas krav. Om en verksamhetsutövare inte kan uppfylla bör-kraven i enlighet med de allmänna råden kan verksamhetsutövaren vidta andra motsvarande åtgärder. Till skillnad från föreskrifter är allmänna råd inte juridiskt bindande.[1]

3 Tillsyn

Cybersäkerhetsförordningen pekar ut ett antal myndigheter som tillsynsmyndigheter. En tillsynsmyndighet ska utöva tillsyn i sin sektor/sina sektorer över att cybersäkerhetslagen och de föreskrifter som har meddelats i anslutning till lagen följs. Tillsynsmyndigheterna ska bland annat bedriva tillsyn om föreskrifterna om säkerhetsåtgärder och ledningens utbildning följs.

NCSC vid FRA leder ett samarbetsforum där tillsynsmyndigheterna ingår. Syftet med forumet är att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn.

4 Föreskrifternas utformning

Föreskrifterna förtydligar CSL:s krav på säkerhetsåtgärder och ledningens utbildning. Kraven på cybersäkerhet är grupperade i organisatoriska, tekniska och driftrelaterade respektive fysiska säkerhetsåtgärder. Det övergripande syftet med föreskrifterna är att säkerställa:

- att verksamhetsutövaren bedriver ett systematiskt och riskbaserat cybersäkerhetsarbete utifrån ett allriskperspektiv[2],
- en miniminivå av cybersäkerhet hos verksamhetsutövare som omfattas av CSL,
- att verksamhetsutövaren utformar sina säkerhetsåtgärder över miniminivån när den egna verksamheten har behov av det.

[1] Myndigheternas föreskrifter (SB PM 2025:4) s. 44 https://www.regeringen.se/contentassets/4a78b51adf5a41b09dc93f2bc2fe2846/myndigheternas-foreskrifter-pm-20254.pdf.

[2] Begreppet ”allriskperspektiv” är ett nyckelbegrepp som förklaras närmare i avsnitt 5.3.

Kraven på säkerhetsåtgärder gällande organisatoriska, driftrelaterade och fysiska säkerhetsåtgärder anger en miniminivå. Genom att bedriva ett systematiskt och riskbaserat arbete i enlighet med 3 kap. skapar verksamhetsutövaren även en förmåga att kunna identifiera och hantera sitt behov av cybersäkerhet över miniminivån.

Vidtagandet av säkerhetsåtgärderna i föreskrifterna ska inte ses som fristående åtgärder eller en "checklista". Verksamhetsutövare behöver förstå sin verksamhet, sina system, sina leveranskedjor och sin omvärld. Den kunskapen gör det möjligt att förstå vilka risker som finns och vilka konsekvenser olika händelser kan få i verksamheten samt samhället i stort. Utifrån den bilden kan säkerhetsåtgärder vidtas, utformas och prioriteras så att de kontinuerligt motsvarar verksamhetens förutsättningar och behov.

Organisatoriska, tekniska, driftrelaterade och fysiska säkerhetsåtgärder kompletterar och förstärker varandra. En teknisk säkerhetsåtgärd, såsom säkerhetsloggning, får exempelvis bättre effekt när den stöds av en tydlig ansvarsfördelning, fungerande arbetssätt, rätt kompetens och tillgängliga resurser. På motsvarande sätt får organisatoriska säkerhetsåtgärder, såsom riskhantering, relevans först när de används för att stärka säkerheten i den digitala miljön.

Eftersom verksamheten, hoten och riskerna förändras över tid kan erfarenheter från den löpande verksamheten, förändringar, övningar, tester och eventuella incidenter ge anledning att se över tidigare bedömningar och anpassa säkerhetsåtgärderna.

När det gäller ledningens utbildning och dess roll i arbetet med cybersäkerhet förtydligar föreskrifterna vilken kunskap och kompetens som ledningen behöver 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.

4.1 Föreskrifternas disposition

Föreskrifterna är strukturerade enligt följande:

- Kapitel 2 innehåller krav på ledningens utbildning om säkerhetsåtgärder.
- Kapitel 3 innehåller krav på organisatoriska säkerhetsåtgärder. Kraven omfattar exempelvis systematiskt och riskbaserat arbete med cybersäkerhet, interna regler och arbetssätt, roller, ansvarsområden och

befogenheter liksom omvärldsbevakning, informationsklassning och riskhantering samt uppföljning och utvärdering.
- Kapitel 4 omfattar krav på tekniska och driftrelaterade säkerhetsåtgärder. Kraven omfattar exempelvis säkerhetskonfigurering, behörighetshantering, övervakning, säkerhetsloggning och logganalys, kryptering samt ändringshantering.
- Kapitel 5 innehåller krav på fysiska säkerhetsåtgärder rörande lokaler och tekniska försörjningssystem.
- Kapitel 6 innehåller sektorsspecifika krav. För närvarande endast riktade till verksamhetsutövare inom offentlig förvaltning. Kraven gäller system för kriskommunikation.
- Kapitel 7 reglerar möjligheterna till undantag från kraven i föreskrifterna.

4.2 Närmare om utformning av kraven

Kraven på en viss säkerhetsåtgärd inleds oftast med en målformulering som tydliggör varför en viss säkerhetsåtgärd ska vidtas. Med ett exempel hämtat från **3 kap. 10 § om omvärldsbevakning**:

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

Av kravet framgår att verksamhetsutövaren ska bedriva omvärldsbevakning med ett visst syfte som ska uppnås.

När det finns skäl har krav på att vidta en viss säkerhetsåtgärd konkretiserats ytterligare. Detta är ett exempel hämtat från samma paragraf:

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.

I exemplet tydliggörs från vilka källor verksamhetsutövaren minst ska inhämta information för sin omvärldsbevakning.

Vissa krav på säkerhetsåtgärder kompletteras med **allmänna råd.** Dessa ger rekommendationer och konkretiserar ytterligare hur verksamhetsutövaren bör uppfylla ”ska-kravet”. När det gäller omvärldsbevakning är de allmänna råden utformade på följande sätt:

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).*

Det allmänna rådet rekommenderar ytterligare källor till information inom ramen för verksamhetsutövarens omvärldsbevakning. Om en verksamhetsutövare inte kan uppfylla bör-kraven i enlighet med de allmänna råden kan verksamhetsutövaren vidta andra åtgärder med motsvarande verkan, i det här fallet använda andra källor för att inhämta motsvarande relevant information.

5 Uttryck och tidsangivelser

I föreskrifterna används några ofta återkommande uttryck för att beskriva på vilket sätt eller inom vilken tidsfrist något ska göras. Dessa förklaras i detta avsnitt. Avsnittet innehåller även begrepp av grundläggande betydelse för förståelse av föreskrifterna. För att underlätta förståelsen av hur begreppen används i föreskrifterna ges förklaringar och exempel.

5.1 Beskrivning av hur krav ska omhändertas

Fastställa:
Begreppet används synonymt med besluta. Exempelvis fastställa interna regler och arbetssätt i 3 kap. 3 §.

Säkerställa:
Begreppet används när verksamhetsutövaren behöver verifiera att något finns eller är på ett visst sätt. Exempelvis ska enligt 3 kap. 8 § systemägaren, i de system denne ansvarar för, säkerställa att risker analyserats och att informationsägarens identifierade nivå av skydd uppnås.

Identifiera och hantera behovet av:
Formuleringen innebär att verksamhetsutövaren aktivt ska analysera och därefter ta ställning till om det finns behov av en viss åtgärd. Identifierat behov ska därefter omhändertas på ett ändamålsenligt sätt. Formuleringen ger verksamhetsutövaren flexibilitet i att själv utforma en säkerhetsåtgärd utifrån externa krav, interna behov och risk. Formuleringen används i exempelvis 3 kap. 12 § (riskhantering) enligt vilken verksamhetsutövaren ska identifiera och hantera behovet av att uppdatera genomförda riskanalyser vid förändrade hot och nya sårbarheter som kan påverka cybersäkerheten.

Om inte uppenbart obehövlig:
Formuleringen används för att beskriva något som ska vidtas, om inte verksamhetsutövaren bedömer att det absolut inte behövs. Som exempel kan nämnas att verksamhetsutövaren enligt 4 kap. 20 § (avseende krav på övervakning, säkerhetsloggning och logganalys) ska, om inte uppenbart obehövligt, ansluta sig till automatiska notifieringar av tekniska sårbarheter (ANTS) hos den nationella CSIRT-enheten[3]. För mer information om ANTS, se avsnitt **Fel! Hittar inte referenskälla.**.

5.2 Tidsfrister

I föreskrifterna används tidsfrister när en åtgärd ska vara utförd. Uttrycken listas utifrån hur snabbt åtgärden ska vidtas. I detta avsnitt förklaras vad som avses med uttrycken.

Tabell 1 - Tidsfrister

Begrepp	Ev. definition	Förklaring
Skyndsamt	*Saknar definition i CSL och tillhörande föreskrifter.*	Åtgärden är prioriterad och ska vidtas snarast.
Utan onödigt dröjsmål	*Saknar definition i CSL och tillhörande föreskrifter.*	Åtgärden vidtas så snart det kan ske.[4]
Inom 72 timmar	*Saknar definition i CSL och tillhörande föreskrifter.*	Åtgärden vidtas så snart det är möjligt, dock senast inom 72 timmar från det att det som föranlett åtgärden gjorts tillgängligt.
Var tredje månad	*Saknar definition i CSL och tillhörande föreskrifter.*	Åtgärden vidtas minst en gång vart tredje månad. Detta innebär dock ingen begränsning av åtgärden och den kan således vidtas med tätare frekvens än så.
Vid behov men minst en gång per år	*Saknar definition i CSL och tillhörande föreskrifter.*	Åtgärden vidtas vid behov. Bedömningen kring när behov föreligger behöver göras från fall till fall. Om behov inte ansetts

[3] CSIRT är en förkortning för ”Computer Security Incident Response Team”. Nationellt cybersäkerhetscenter vid FRA är Sveriges nationella CSIRT.
[4] Prop. 2025/26:28 Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag, s. 119

Begrepp	Ev. definition	Förklaring
		föreligga ska åtgärden genomföras minst en gång per år.
Acceptabla tider för otillgänglighet och bristande funktionalitet	*Saknar definition i CSL och tillhörande föreskrifter.*	Denna tidsram ska vara sådan inom vilken otillgänglighet och bristande funktionalitet är acceptabel. Vad som utgör acceptabla tider för otillgänglighet och bristande funktionalitet för informationsbehandlingen bestämmer verksamhetsutövaren utifrån exempelvis externa krav, interna behov och identifierade risker.

5.3 Grundläggande begrepp

Följande begrepp är av grundläggande betydelse för förståelse av föreskrifterna. Begreppen har delats in i följande kategorier:

1. nyckelbegrepp,
2. roller,
3. uttryck med särskild koppling till verksamhetsutövarens digitala miljö,
4. övriga uttryck.

Tabell 2 - Nyckelbegrepp

Begrepp	Ev. definition	Förklaring och exempel
Allriskperspektiv	*Saknar definition i CSL och tillhörande föreskrifter.*	Allriskperspektivet innebär att verksamhetsutövare ska sträva efter att bedöma alla risker för systemen som ska skyddas och att analysera alla möjliga orsaker till att en risk realiseras.[5] Både medvetet illvilligt handlande och misstag räknas in. Det kan vara organisatoriska, tekniska och driftrelaterade risker och fysiska risker samt cyberhot. Som exempel kan nämnas väder- och klimatrelaterade risker, brand i datacenter, systemfel på grund av felkonfiguration eller utpressningsangrepp.

[5]Prop. 2025/26:28 s. 244.

Begrepp	Ev. definition	Förklaring och exempel
System	*Uttrycket framgår av 1 kap. 2 § p.16 CSL:* *nätverks- och informationssystem: i cybersäkerhetslagens mening, dvs nätverks- och informationssystem:* *a) ett elektroniskt kommunikationsnät enligt 1 kap. 7 § lagen om elektronisk kommunikation,* *b) en enhet eller en grupp enheter som är sammankopplade eller hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av digitala uppgifter, eller* *c) digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana hjälpmedel som omfattas av a och b för att de ska kunna användas, skyddas och underhållas*	En förkortning av nätverks- och informationssystem enligt 1 kap. 2 § p.16. CSL. Nätverk- och informationssystem (system i föreskrifterna) kan mycket förenklat sägas utgöras av följande: 1) Elektroniska kommunikationsnät, 2) En eller flera sammankopplade datorer, eller 3) Digitala uppgifter som på något sätt hanteras i 1) eller 2). System kan vara av många olika slag. Som exempel kan nämnas system för hantering av fakturor, löner (it-system) och styrning av dammar, energiförsörjning, dricksvattenförsörjning och transporter (ot-system).
Cybersäkerhet	Uttrycket definieras i 1 kap. 2 § 5 CSL[6] som: *all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system*	Begreppet cybersäkerhet har i andra sammanhang ibland haft en snävare betydelse med större tekniskt fokus, närmare det som brukar benämnas it-säkerhet. Ibland har begreppet använts för att beskriva endast skydd mot antagonistiska hot. Den legaldefinition som nu har fastslagits av EU innebär i stället att cybersäkerhet har

[6] Uttrycket definieras på samma sätt som i artikel 2.1 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 526/2103 (cybersäkerhetsakten).

Begrepp	Ev. definition	Förklaring och exempel
	och andra berörda personer mot cyberhot	fått en innebörd som i stort kan likställas med det som traditionellt beskrivs som informationssäkerhet.[7] Exempelvis organisatoriska, tekniska och driftrelaterade samt fysiska åtgärder som behövs för att skydda system mot cyberhot.
Cyberhot	Definieras i 1 kap. 2 § 4 CSL som [8]: *en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informations-system, användare av dessa system och andra personer.*	Cyberhot kan delas in i tre huvudsakliga kategorier: • Mänskliga hot (kan vara både antagonistiska hot i form av angrepp och icke-antagonistiska hot i form av misstag). • Tekniska hot (i form av systemfel). • Naturhot (som till exempel väderfenomen, jordbävningar) Samtliga hot kan leda till incidenter som kan påverka cybersäkerheten och leda till allvarliga konsekvenser för både enskilda och organisationer.
Sektorsverksamhet	Definierat i 1 kap. 4 § MCFFS 2026:11: *sådan verksamhet som omfattas av cybersäkerhetslagen*	Som utgångspunkt gäller CSL:s regler hela verksamhetsutövarens organisation och all verksamhet som verksamhetsutövaren bedriver.[9] Den verksamhet som är anledningen till att man som organisation omfattas av CSL benämns i föreskrifterna sektorsverksamhet. En verksamhetsutövare kan bedriva både sektorsverksamhet och annan verksamhet, exempelvis är hälso- och sjukvård sektorsverksamhet medan att bedriva lunchrestauranger bedöms som annan verksamhet. I föreskrifterna ställs i vissa fall något skarpare krav på incidentrapportering

[7] Prop. 2025/26:28 s. 40.
[8] Uttrycket definieras på samma sätt som i artikel 2.8 i cybersäkerhetsakten.
[9] Det finns undantag för lagens tillämpning enligt 1 kap. 12 § CSL, bland annat för verksamhetsutövare som bedriver säkerhetskänslig verksamhet.

Begrepp	Ev. definition	Förklaring och exempel
		eller att vidta säkerhetsåtgärder i sektorsverksamhet.
Viktiga samhällsfunktioner	Definierat i 1 kap. 4 § MCFFS 2026:11: *en samhällsfunktion som är nödvändig för samhällets grundläggande behov, värden eller säkerhet.*	Begreppet används när det är viktigt att förstå och tydliggöra hur den egna verksamheten och systemen påverkar samhällets funktionalitet. De viktiga samhällsfunktionerna är en utgångspunkt för samhällets arbete med beredskapsarbete. Kunskap om hur cybersäkerhet i den egna verksamheten bidrar till att upprätthålla viktiga samhällsfunktioner[10] stärker arbetet med civilt försvar.

Tabell 3 - Roller

Begrepp	Ev. definition	Förklaring och exempel
Verksamhetsutövare	Definierat i 1 kap. 3–8 §§ CSL.	Den som omfattas av CSL.
Ledning	*Saknar definition i CSL och tillhörande föreskrifter.*	En bedömning av vem som anses ingå i ledningen behöver göras från fall till fall då det skiljer sig åt beroende på aktuell verksamhetsutövares verksamhetsform. För aktiebolag och ekonomiska föreningar avser ledningen styrelsen och verkställande direktör samt ersättare för dessa. För handelsbolag och enkla bolag är bolagsmännen ansvariga för förvaltningen och är således att betrakta som ledningen. För myndigheter som står under

[10] För ytterligare underlag rörande viktiga samhällsfunktioner hänvisas till MCF: https://www.mcf.se/sv/amnesomraden/beredskap-for-kris-och-krig/beredskap-for-aktorer/samhallsviktig-verksamhet/viktiga-samhallsfunktioner/.

Begrepp	Ev. definition	Förklaring och exempel
		regeringen är ledningen den som framgår av myndighetens instruktion eller annan författning. För kommuner och regioner utgörs ledningen av kommun- respektive regionstyrelsen.[11]
Samordnare	*Saknar definition i CSL och tillhörande föreskrifter.*	En eller flera roller eller funktioner hos verksamhetsutövaren med ansvar för samordning av verksamhetsutövarens cybersäkerhetsarbete. Notera att rollen eller funktionen inte specifikt behöver benämnas som "samordnare" i verksamhetsutövarens organisation. I NCSC:s stöd benämns denna roll oftast CISO, den kan även exempelvis kallas informationssäkerhetssamordnare eller informationssäkerhetschef. [12]
Informationsägare	*Saknar definition i CSL och tillhörande föreskrifter.*	En eller flera roller eller funktioner hos verksamhetsutövaren med ansvar för informationsbehandling i system. Notera att rollen inte specifikt behöver benämnas som "informationsägare" i verksamhetsutövarens organisation.[13]
Systemägare	*Saknar definition i CSL och tillhörande föreskrifter.*	En eller flera roller eller funktioner hos verksamhetsutövaren med ansvar för säkerheten i system. Notera att rollen inte specifikt behöver benämnas som "systemägare" i verksamhetsutövarens organisation.[14]

Tabell 4 - Begrepp kopplade till verksamhetsutövarens digitala miljö

Begrepp	Ev. definition	Förklaring och exempel
Digital miljö	Definieras i 1 kap. 4 § MCFFS 2026:11:	Verksamhetsutövarens samtliga system, det vill säga både de som används för den interna verksamheten och externa tjänster som

[11] Prop. 2024/25:28, s. 99f.
[12] Myndigheten för civilit försvar, Konsekvensutredning rörande Myndigheten för civilt försvar, Konsekvensutredning avseende föreskrifter och allmänna råd om säkerhetsåtgärder och ledningens utbildning för väsentliga och viktiga verksamhetsutövare, (Konsekvensutredning) s. 41.
[13] Konsekvensutredning s. 41.
[14] Konsekvensutredning s. 41.

Begrepp	Ev. definition	Förklaring och exempel
	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.	verksamhetsutövaren tillhandahåller. Det inkluderar utkontrakterad informationsbehandling.
Utkontrakterad informationsbehandling	*Saknar definition i CSL och tillhörande föreskrifter.*	Begreppet utkontrakterad informationsbehandling avser alla typer av tjänster som en verksamhetsutövare har anlitat en leverantör för, såsom drift- och molntjänster, ekonomitjänster, systemutveckling, säkerhet med flera. Verksamhetsutövaren kan utkontraktera informationsbehandling i hela eller delar av sin digitala miljö till en leverantör.
Sektorskritiskt system	Definieras i 1 kap. 4 § MCFFS 2026:11: *ett system som är nödvändigt för att kunna bedriva intern verksamhet eller tillhandahålla externa tjänster inom sektorsverksamhet,*	Verksamhetsutövaren behöver själv bedöma vilka system som är sektorskritiska inom dennes sektorsverksamhet. Sektorskritiska system innefattar sådana system som är nödvändiga för att verksamhetsutövaren långsiktigt ska kunna bedriva den sektorsverksamhet som specificeras i CSL. Det omfattar både system som används i tjänster som tillhandahålls externt och system som används internt om deras funktionalitet är central för att sektorsverksamheten ska kunna bedrivas enligt normalläge.
Information i behov av utökat skydd	Definieras i 1 kap. 4 § MCFFS 2026:11:	Information i behov av utökat skydd på grund av externa krav kan ha sin grund i annan reglering eller avtal som verksamhetsutövaren ingått med andra

Begrepp	Ev. definition	Förklaring och exempel
	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.	organisationer. Exempel på detta kan vara hantering av personuppgifter enligt dataskyddsförordningen (GDPR) eller regler för att skydda företagshemligheter enligt lagen (2018:558) om företagshemligheter. Verksamhetsutövaren kan också vid sin informationsklassning identifiera information i behov av utökat skydd.
Segment	*Saknar definition i CSL och tillhörande föreskrifter.*	Avser en indelning av digital miljö i olika nätverkssegment för att förhindra spridning och minimera konsekvenser av incidenter.
Ot-segment	*Definieras i 1 kap. 4 § MCFFS 2026:11:* *ett nätverkssegment som är inrättat för cyberfysiska system.*	Nätverkssegment i den digitala miljön som verksamhetsutövaren har inrättat för system som används för att styra och övervaka fysiska enheter, fysiska processer och fysiska händelser. Sådana system kallas cyberfysiska system eller ot system (ot är en förkortning för operativ teknik).
It-segment	Definieras i 1 kap. 4 § MCFFS 2022:11: *ett nätverkssegment som är inrättat för andra system än sådana system som placeras i ot- segment,*	Nätverkssegment som är inrättat för it-system. It-segment kan ha olika storlek och syften. I it-segment gäller föreskrifternas ordinarie krav på säkerhetsåtgärder, inte de anpassningar som gäller för ot-segment.
Produktionsmiljö	Definieras i 1 kap. 4 § MCFFS 2026:11: *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*	Produktionsmiljön används för verksamhetsutövarens ordinarie verksamhet, både sektorsverksamhet och annan verksamhet. Innehåller typiskt sett it- och, vid behov, ot-segment för systemadministration, centrala systemsäkerhetsfunktioner verksamhetssystem och externt exponerade

Begrepp	Ev. definition	Förklaring och exempel
	av it-segment och ot-segment.	system. Kan även innehålla segment som används för andra uppgifter.
Utvecklingsmiljö	*Saknar definition i CSL och tillhörande föreskrifter.*	En avskild del av den digitala miljön som verksamhetsutövaren använder för utvecklingsarbete som bedöms kunna påverka säkerheten i produktionsmiljön, exempelvis utveckling av mjukvara till produktionsmiljön.
Testmiljö	*Saknar definition i CSL och tillhörande föreskrifter.*	En avskild del av den digitala miljön som verksamhetsutövaren använder för att testa system där testningen bedöms kunna påverka säkerheten i produktionsmiljön, exempelvis test av nyutvecklad mjukvara eller förändrad konfiguration av system.
Utbildningsmiljö	*Saknar definition i CSL och tillhörande föreskrifter.*	En avskild del av den digitala miljön som verksamhetsutövaren använder för intern utbildning av egna användare där utbildningen bedöms kunna påverka säkerheten i produktionsmiljön, exempelvis utbildning på ny eller uppdaterad mjukvara till produktionsmiljön. All utbildningsverksamhet bedrivs inte i utbildningsmiljön. Utbildning som en verksamhetsutövare exempelvis tillhandahåller externa aktörer som en del av sin sektorsverksamhet bedrivs i produktionsmiljön eftersom det hör till verksamhetsutövarens ordinarie verksamhet.

Tabell 5 Övriga uttryck

Begrepp	Ev. definition	Förklaring och exempel
Externa krav, interna behov och identifierade risker	*Saknar definition i CSL och tillhörande föreskrifter.*	Formuleringen externa krav, interna behov och identifierade risker används i föreskrifterna för att beskriva olika typer av ingångsvärden som föranleder behov av cybersäkerhet. Exempel på externa krav är författningskrav eller krav som en extern aktör ställer i avtal. Det kan vara exempelvis hantering av personuppgifter eller sekretess för företagshemligheter. Med interna

Begrepp	Ev. definition	Förklaring och exempel
		behov avses den egna verksamhetens behov. Det kan vara exempelvis att en verksamhetsutövare för att kunna utföra en viss typ av informationsbehandling behöver ha en mycket hög tillgänglighet till vissa system vilket i sin tur förutsätter att lämpliga säkerhetsåtgärder vidtas. Vilka risker som verksamhetsutövaren identifierat ska användas som ingångsvärde vid utformningen och införandet av säkerhetsåtgärder.
Lämpliga och proportionerliga säkerhetsåtgärder	*Saknar definition i CSL och tillhörande föreskrifter.*	Säkerhetsåtgärder som vidtas ska bland annat vara lämpliga och proportionella. Säkerhetsåtgärderna ska säkerställa en nivå på säkerheten i system som är lämplig i förhållande till den föreliggande risken, med beaktande av vissa standarder och genomförandekostnader. Vid bedömningen av säkerhetsåtgärders proportionalitet ska vederbörlig hänsyn tas till verksamhetsutövarens grad av riskexponering, verksamhetsutövarens storlek samt sannolikheten för att incidenter inträffar och deras allvarlighetsgrad, inbegripet deras samhälleliga och ekonomiska konsekvenser. Det behöver ske separata bedömningar när det gäller lämplighet och proportionalitet. Det kan således finnas säkerhetsåtgärder som är proportionella men inte lämpliga. Lämpligheten handlar om att vidta rätt åtgärd i förhållande till en viss risk, medan proportionaliteten handlar om hur omfattande åtgärden måste vara för att motverka eller eliminera risken. Båda dessa bedömningar ska göras.
Konfidentialitet	*Saknar definition i CSL och tillhörande föreskrifter.*	Egenskap som innebär att information inte tillgängliggörs eller avslöjas för obehöriga individer, objekt eller processer (Svensk ANM. I Terminologi för informationssäkerhet (SIS-TR 50) definieras ”konfidentialitet” som ’skydd mot obehörig insyn’).
Riktighet	*Saknar definition i CSL och tillhörande föreskrifter.*	Egenskap som innebär att vara korrekt och fullständig (Svensk ANM. Enligt svensk terminologi för informationssäkerhet (SIS-TR

Begrepp	Ev. definition	Förklaring och exempel
		50) definieras ”riktighet” som ’skydd mot oönskad förändring’).
Autencitet	*Saknar definition i CSL och tillhörande föreskrifter.*	Överensstämmelse mellan faktisk och påstådd identitet och meddelandens ursprung. Den tekniska process vari äktheten, autenticiteten bekräftas kallas autentisering. Denna kontroll kan exempelvis avse användare, processer, systemkomponenter och informationsobjekt.
Tillgänglighet	*Saknar definition i CSL och tillhörande föreskrifter.*	Egenskapen att vara åtkomlig och användbar på begäran av ett behörigt objekt (Svensk ANM. I Terminologi för informationssäkerhet (SIS-TR 50) definieras ”tillgänglighet” som ’åtkomst för behörig person vid rätt tillfälle’).
Klient	*Saknar definition i CSL och tillhörande föreskrifter.*	En enhet eller ett program som hämtar information eller tjänster från en server.
Realtidsövervakning	*Saknar definition i CSL och tillhörande föreskrifter.*	Innebär kontinuerlig och automatisk kontroll av servrar, nätverk och applikationer för att upptäcka avvikelser och säkerhetshot. Utförs ofta med stöd av så kallade soc-tjänster.
Interna regler och arbetssätt		Vad en verksamhetsutövare använder för benämningar på sin interna styrning av organisationen kan skilja sig åt. Det kan handla om riktlinjer, rutiner mm. Föreskrifternas krav på interna regler och arbetssätt innebär inte någon skyldighet att ändra namnet på dessa till interna regler och arbetssätt. Vilka interna regler och arbetssätt som behöver fastställas ska utgå från verksamhetsutövarens behov av att inrikta cybersäkerhetsarbetet i organisationen. För att genomföra många av de säkerhetsåtgärder som regleras i föreskrifterna förutsätts att det finns interna regler och arbetssätt som stöd för arbetet. I de allmänna råden tydliggörs vad interna regler och arbetssätt bör tydliggöra för att kunna vara ett ändamålsenligt stöd för verksamhetsutövaren.
Informationsbehandling	*Saknar definition i CSL och tillhörande föreskrifter.*	Insamling, överföring, lagring, bearbetning, visning, användning eller radering av information i system. I ot-segment omfattar

Begrepp	Ev. definition	Förklaring och exempel
		begreppet även digital behandling av signaler, mätvärden, styrkommandon, larm, konfigurationer och annan data som används för att styra, övervaka eller påverka fysiska processer.

6 Andra kapitlet Ledningens utbildning

6.1 Ledningens utbildning 2 kap. 1 §

6.1.1 Introduktion

I ett systematiskt och riskbaserat arbete med cybersäkerhet har ledningen en central roll för att arbetet ska kunna bedrivas på avsett sätt. Brister avseende ledningens engagemang i arbetet utgör en sedan länge och ofta påtalad utmaning för, och anledning till, organisationers möjlighet att bedriva ett systematiskt och riskbaserat cybersäkerhetsarbete och därmed möjlighet att uppnå en ändamålsenlig cybersäkerhet. Precis som för andra utgör en ändamålsenlig utbildning en förutsättning för ledningen att kunna utföra sina uppgifter. Ledningen behöver få tillräckligt med kunskap och kompetens för att kunna utföra sina uppgifter som de ansvarar för, det vill säga godkänna och övervaka säkerhetsåtgärderna.

Bristande utbildning kan göra det svårt för ledningen att utföra sina uppgifter enligt cybersäkerhetslagen. Vikten av ledningens arbete visar sig även genom att cybersäkerhetslagen ger en tillsynsmyndighet rätt att under vissa förhållanden besluta att en befattningshavare inte längre får ha en ledningsfunktion.

6.1.2 Krav

2 kap. 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.

6.1.3 Tolkningsstöd

Begrepp och formuleringar

För tolkningsstöd rörande begreppen sektorsverksamhet och viktiga samhällsfunktioner, se Begreppslistan i inledningen.

Ledningen

Av cybersäkerhetslagens 2 kap. 4 § framgår att de personer som ingår i ledningen för en verksamhetsutövare ska genomgå utbildning om säkerhetsåtgärder.

För ett aktiebolag avses med ledningen primärt styrelsen, den verkställande direktören och ersättare för dessa. Motsvarande gäller för ekonomiska föreningar medan det för handelsbolag är bolagsmännen som utgör ledningen. Vad som utgör ledningen enligt cybersäkerhetlagen tolkas på samma sätt som i 2 § myndighetsförordningen (2007:515). För statliga myndigheter är huvudregeln är att en myndighet under regeringen leds av en myndighetschef om det är en enrådighetsmyndighet, en styrelse om det är en styrelsemyndighet och en nämnd om det är en nämndmyndighet. Myndighetens ledningsform anges i myndighetens instruktion eller i någon annan författning. I kommuner och regioner utgörs ledningen av kommun- respektive regionstyrelsen i enlighet med 6 kap. 1 § kommunallagen.

Verksamhetsutövare kan ha byggt upp arbetet på olika sätt och personer i ledande positioner som inte ingår i de grupper som pekas ut som ledning i cybersäkerhetslagens mening kan ändå ha en central ledande position hos verksamhetsutövaren som innefattar att övervaka och godkänna säkerhetsåtgärder. Deras utbildningsbehov regleras i 3 kap. 9 § i föreskrifterna.

Innehåll och omfattning

Utbildningen ska bland annat syfta till att ledningen ska ha tillräcklig kunskap och kompetens för att kunna identifiera risker och bedöma vilka säkerhetsåtgärder som bör vidtas av verksamhetsutövaren. Vad utbildningen närmare ska omfatta och vilka moment som ska ingå kan variera bland annat utifrån vilken verksamhet som bedrivs. Det övergripande syftet är att ge ledningen rätt förutsättningar för att utföra sina uppgifter.

Ledningen hos olika verksamhetsutövare kan ha mycket skilda utgångspunkter, allt från att vara djupt insatta i cybersäkerhetsfrågor till att området i det närmaste är nytt. Regleringen ger dock inte något utrymme för att inte genomföra någon utbildning alls. Ledningens förkunskaper, önskemål och arbetssätt är centrala ingångsvärden vid utformningen för att utbildningen ska vara relevant. Eftersom de mer detaljerade kraven på innehåll och utformning är i form av allmänna råd har verksamhetsutövaren en flexibilitet att utforma utbildningen för att motsvara sina behov.

Eftersom förutsättningarna för cybersäkerhet förändras över tid behöver

- utbildningens innehåll ses över vid behov. Sådan översyn skulle kunna föranledas av exempelvis större förändring i ledningsstruktur eller organisation, större förändringar vad gäller hot och risker respektive regelverk.
- utbildningen genomföras återkommande med ett för verksamhetsutövaren lämpligt intervall som uppfyller ledningens behov. Här behöver även behovet av att utbilda nytillträdda deltagare i ledningen beaktas.

Ledningens behov av djupgående tekniska kunskaper i de flesta fall är begränsat. Det kan dock vara lämpligt med en övergripande förståelse för vilka särskilda förutsättningar som användningen av operativ teknik (ot) i verksamheten kan få för cybersäkerhetsarbetet. Exempelvis när sådan teknik används för att styra dammar, eltransmission eller liknande.

Upprätthålla sektorsverksamhet och viktiga samhällsfunktioner

I de allmänna råden rekommenderas bland annat att ledningens utbildning bör omfatta vilken betydelse cybersäkerheten hos verksamhetsutövaren har för att upprätthålla sektorsverksamhet och viktiga samhällsfunktioner. Syftet är att underlätta förståelsen för vilken roll den egna verksamhetens cybersäkerhet spelar för samhällets funktionalitet och i förlängningen totalförsvaret. De viktiga samhällsfunktionerna utgör grunden för aktörers beredskapsarbete och för att identifiera samhällsviktig verksamhet inklusive sådan som än nödvändig för totalförsvaret. Läs mer om de viktigaste samhällsfunktionerna hos Myndigheten för civilt försvar (MCF).

6.1.4 Kopplingar till andra paragrafer

- Närmare om vad som ingår i ledningens uppgifter framgår bland annat av föreskrifterna 3 kap. 4 § (se avsnitt 7.3).
- Krav på utbildning för ledningspositioner som inte utgör ledning i cybersäkerhetslagens mening regleras i föreskrifterna 3 kap 9 § (se avsnitt 7.4).

7 Tredje kapitlet Organisatoriska säkerhetsåtgärder

7.1 Systematiskt och riskbaserat arbete med cybersäkerhet 1–2 §§

7.1.1 Introduktion

Arbetet med informationssäkerhet behöver vara strukturerat och systematiskt för att bli effektivt. Den snabba utvecklingen inom informationshantering motiverar detta ytterligare, eftersom det ständigt kommer nya hot, nya tekniska möjligheter och förändrade lagkrav. Det räcker inte att införa ett antal säkerhetsåtgärder och se cybersäkerhetsarbetet som färdigt. Det är en säkerhetsåtgärd i sig att regelbundet se över andra införda säkerhetsåtgärders effektivitet så att säkerheten över tid är anpassad till verksamhetsutövarens utveckling och förändringar i omvärlden. Ett systematiskt och riskbaserat cybersäkerhetsarbete involverar hela organisationen.

Uteblivet systematiskt och riskbaserat arbete kan både leda till säkerhetshål och ett för kraftigt skydd som inte motsvarar verksamhetens behov.

7.1.2 Krav

3 kap. 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.

3 kap. 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.

7.1.3 Tolkningsstöd

Begrepp och formuleringar

För tolkningsstöd rörande begreppen allriskperspektiv, identifiera och hantera, externa krav, interna behov och identifierade risker, se Begreppslistan i inledningen.

Ett systematiskt och riskbaserat cybersäkerhetsarbete

Ett systematiskt cybersäkerhetsarbete innebär enligt cybersäkerhetslagens förarbeten att arbetet bland annat ska bedrivas långsiktigt, kontinuerligt och metodiskt. Med risk avses enligt artikel 6.9 i NIS 2-direktivet risk för förlust eller störning orsakad av en incident, som ska uttryckas som en kombination av omfattningen av förlusten eller störningen och sannolikheten för att en sådan incident inträffar. Att bedriva cybersäkerhetsarbetet på ett systematiskt och riskbaserat sätt innebär att verksamhetsutövaren har förmåga att på ett strukturerat sätt löpande anpassa och utveckla säkerhetsåtgärder utifrån externa krav, interna behov och identifierade risker.

För att uppnå en hög nivå av cybersäkerhet i samhället finns det dessutom ett behov av att säkerställa att verksamhetsutövarna som omfattas av CSL har en miniminivå av cybersäkerhet. Med anledning av detta kompletteras det mer övergripande kravet på att cybersäkerhetsarbetet bedrivs systematiskt och riskbaserat med mer detaljerade krav i övriga delar i regleringen på utformningen av respektive säkerhetsåtgärd. Sådan konkretisering görs både för de olika organisatoriska säkerhetsåtgärderna som direkt ingår i ett systematiskt och riskbaserat arbetssätt (informationsklassning, omvärldsbevakning, uppföljning med mera) och för övriga säkerhetsåtgärder såsom segmentering och kontinuitetshantering.

Det åligger verksamhetsutövaren att genomgående anpassa respektive säkerhetsåtgärd till sina egna behov där dessa behov innebär en högre nivå av cybersäkerhet än den lägsta-nivå som anvisas i föreskrifterna. Genom det systematiska och riskbaserade cybersäkerhetsarbetet skapas förutsättningar för verksamhetsutövaren att identifiera och hantera sina egna behov av cybersäkerhet.

Integrera arbetet med befintligt sätt att leda och styra organisationen

Kravet syftar till att säkerställa att cybersäkerhetsarbetet är integrerat i ordinarie sätt att leda och styra organisationen, såsom budgetarbete, verksamhetsplanering och beslutsprocesser. Arbetet med ett systematiskt och riskbaserat cybersäkerhetsarbete bör bedrivas kontinuerligt. Om det passar organisationen kan verksamhetsutövare välja att inkorporera målen för sitt cybersäkerhetsarbete i en gemensam säkerhetspolicy.

Standarder

I de fall verksamhetsutövaren har identifierat ett behov av att använda standarder i sitt cybersäkerhetsarbete behöver motsvarande bedömning göras kring vilka standarder som ska användas. Det allmänna rådet ger ett antal exempel på standarder som lämpar sig för systematiskt och riskbaserat arbete, men ger inte en uttömmande lista på standarder som kan användas för detta. Bedömningen kring vilken standard som lämpligen kan användas för att uppfylla identifierat syfte behöver göras av verksamhetsutövaren.

Som stöd för arbete kring ot-segment kan exempelvis följande eller motsvarande standarder användas:

- Svensk standard SS-EN IEC 62443-2-1 Fordringar på OT-säkerhetsprogram för tillgångar i industriella automationssystem
- Svensk standard SS-EN 62443-3-2 IT-säkerhet i industriella automationssystem - Del 3-2: Riskbedömning och systemkonstruktion
- Svensk standard SS-EN 62443-3-3 IT-säkerhet i industriella automationssystem - Del 3-3: IT-säkerhet i nät och system - Fordringar på systemets säkerhet och på säkerhetsnivåer

7.1.4 Kopplingar till andra paragrafer

Närmare om:

- Interna regler och arbetssätt, 3 kap. 3 § (se avsnitt 7.2).
- Roller och ansvarsområden 3 kap. 4–8 §§ (se avsnitt 7.3)
- Informationsklassning, 3 kap. 11 § (se avsnitt 7.4)
- Riskhantering, 3 kap. 12–13 §§ (se avsnitt 7.5).
- Uppföljning och utvärdering, 3 kap. 19 § (se avsnitt 7.9).

7.2 Interna regler och arbetssätt 3 kap. 3 §

7.2.1 Introduktion

Tydliga interna regler och arbetssätt är en grundläggande förutsättning för ett effektivt cybersäkerhetsarbete. Genom att fastställa ansvar, befogenheter och processer för säkerhetsrelaterade aktiviteter säkerställs att rätt åtgärder

genomförs vid rätt tidpunkt och att cybersäkerhetsarbetet bedrivs på ett enhetligt och systematiskt sätt.

Brister i styrning, ansvarsfördelning eller etablerade arbetssätt kan leda till otydlighet kring vem som ansvarar för olika säkerhetsuppgifter, vilket ökar risken för att säkerhetsåtgärder uteblir, incidenter hanteras bristfälligt, risker inte omhändertas och att verksamhetens samlade säkerhetsförmåga försvagas.

7.2.2 Krav

3 kap. 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 ansvarområden 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.

7.2.3 Tolkningsstöd

Begrepp och förklaringar

För tolkningsstöd rörande begreppen interna regler och arbetssätt, externa krav, interna behov och identifierade risker, cybersäkerhet, lämpliga och proportionella säkerhetsåtgärder, se Begreppslistan i inledningen.

Kommunikation till berörd personal

För att verksamhetsutövarens personal ska kunna arbeta systematiskt med cybersäkerhet krävs att dessa känner till de interna regler och arbetssätt som finns. Vilka delar som anses vara relevanta beror på vilken roll eller funktion mottagaren av informationen innehar.

Dokumentation

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. Sådana underlag underlättar för den verksamhetsutövare som står under tillsyn att påvisa att denne genomfört vissa åtgärder men även för en tillsynsmyndighet att bedöma om och hur en verksamhetsutövares cybersäkerhetsarbete utvecklas. Relevant dokumentation bör sparas i minst 7 år från det att handlingen tillkommit. Verksamhetsutövaren kan även spara dokumentationen längre än så om behov anses föreligga.

Dokumentationskravet konkretiseras ytterligare när det gäller driftrelaterad dokumentation i 4 kapitlet.

Det kan även finnas andra anledningar till dokumentation. Dokumentation rörande i vilken utsträckning personal tagit del av exempelvis utbildning eller informationsinsatser kan ibland vara av betydelse för vidtagande av arbetsrättsliga åtgärder vid exempelvis allvarligare regelbrott.

7.2.4 Kopplingar till andra paragrafer

Närmare om:

- Roller, ansvarsområden och befogenheter 3 kap. 4–8 §§ (se avsnitt 7.3)
- Uppföljning och utvärdering 3 kap. 19 § (se avsnitt 7.9).
- Driftrelaterad dokumentation 4 kap. 8 – 10 §§ (se avsnitt 8.3).

7.3 Roller, ansvarsområden och befogenheter 3 kap. 4–8 §§

7.3.1 Introduktion

En tydlig fördelning av roller, ansvarsområden och befogenheter är en grundläggande förutsättning för ett effektivt cybersäkerhetsarbete. Genom att klargöra vem som ansvarar för styrning, riskhantering, säkerhetsåtgärder, incidenthantering och uppföljning säkerställs att cybersäkerhetsarbetet bedrivs systematiskt och att beslut kan fattas och verkställas på rätt nivå i organisationen.

Brister i ansvarsfördelning och befogenheter kan leda till otydlighet, dubbelarbete eller att viktiga säkerhetsuppgifter inte genomförs, vilket ökar risken för säkerhetsbrister, fördröjd incidenthantering, felaktiga beslut och en försvagad säkerhetsförmåga.

7.3.2 Krav

3 kap. 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.

3 kap. 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.

3 kap. 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.

3 kap. 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.

3 kap. 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.

7.3.3 Tolkningsstöd

Begrepp

För tolkningsstöd rörande begreppen lämpliga och proportionella säkerhetsåtgärder, säkerställa, ledning, samordnare, informationsägare, systemägare, vid behov men minst en gång per år, konfidentialitet, riktighet inklusive autenticitet, och tillgänglighet, acceptabla tider för otillgänglighet och bristande funktionalitet, se Begreppslistan i inledningen.

Ledningen

Det framgår av cybersäkerhetslagens förarbeten att det ingår i ledningens uppgifter att godkänna och övervaka genomförandet av säkerhetsåtgärder.[1] Vilka som anses som ledning i cybersäkerhetslagens mening redovisades i avsnittet om ledningens utbildning, avsnitt 6.1. Alla verksamheter är organiserade på olika sätt och arbetet som utförs av en verksamhetsutövares ledning ser inte alltid ut såsom det definieras i cybersäkerhetslagen. Föreskriftskravet är därför utformat för att ge flexibilitet. Detta görs genom att verksamhetsutövarens ledning enligt 3 kap. 4 § ska *säkerställa* att vissa saker görs, det vill säga de behöver inte nödvändigtvis göra det själva utan ska skapa förutsättningar för att rätt nivå i organisationen kan utföra de uppgifter som ingår i att godkänna och övervaka säkerhetsåtgärder.

För att verksamhetsutövare ska kunna arbeta systematiskt och riskbaserat med cybersäkerhet krävs att det finns tydliga mål och inriktning för arbetet. Vid bedömningen av hur dessa mål ska utformas bör verksamhetens behov och risk beaktas. Det finns således inget rätt eller fel svar på vad som utgör lämpligt mål och inriktning, så länge regleringens krav uppfylls. Det kan exempelvis vara så att en organisation som arbetar systematiskt med cybersäkerhet och redan har

en relativt hög sådan sätter högre mål än en organisation som nyligen inlett arbetet med cybersäkerhet och kanske därav väljer att inrikta cybersäkerhetsarbetet med syfte att uppnå den miniminivå som föreskriftskraven ger uttryck för. Mål och inriktning uttrycks ofta i en informationssäkerhetspolicy. Det finns inga hinder för att mål och inriktning för cybersäkerhetsarbetet ingår i en mer omfattande policy, exempelvis för organisationens säkerhetsarbete i stort.

Ledningens roll i cybersäkerhetsarbetet ska tydliggöras, detta gäller både i förhållande till de som inkluderas i ledningen, och för verksamhetsutövarens personal och organisation som helhet.

Resurser för att bedriva ett systematisk och riskbaserat cybersäkerhetsarbete utifrån utsatta mål och inriktning inkluderar såväl personella som ekonomiska resurser.

För att arbetet med cybersäkerhet ska kunna bedrivas effektivt krävs att de roller och ansvarsområden som cybersäkerhetsarbetet kräver har tillräckliga befogenheter och resurser för att utföra tilldelade uppgifter. Stöd för utformningen av befogenheter och tilldelning av resurser finns i avsnittet Roller, ansvarsområden och befogenheter i 3 kap. 4 – 8 §§. Här ska även utformningen av verksamhetsutövarens organisation och hur arbetet med cybersäkerhet fördelas och utformas inom organisationen beaktas.

För att ledningen i cybersäkerhetslagens mening ska kunna *säkerställa* att det beslutas om mål, inriktning och mandat samt tilldelning av tillräckliga resurser och dess mandat, krävs att ledningen har kunskap om verksamhetsutövarens cybersäkerhetsarbete. Det är en uppgift för ledningen att säkerställa att den får den information den behöver om hur arbetet med cybersäkerhet går och vilka behov och utmaningar som verksamhetsutövaren har. Det är samordnaren som har i uppgift att sammanställa informationen. Vilken information som ledningen behöver skiljer sig mellan verksamhetsutövare och beror på respektive organisation men stöd för bedömningen kan hämtas från de allmänna råden till 3 kap. 6 § samt kraven på uppföljning och utvärdering i 3 kap. 19 §.

Kravet på att ledningen ska bli informerad gäller ledningen i cybersäkerhetslagens mening. I det fall som ledningen har delegerat det faktiska arbetet med att leda och övervaka cybersäkerhetsarbetet till en eller flera andra konstellationer hos verksamhetsutövaren följer motsvarande. Det innebär att dessa får del av den information som krävs för uppdraget, vilket följer av bland annat kravet på informationsinsatser mm i 3 kap. 9 § och uppföljning och utvärdering i 3 kap. 19 §. Detta kan bli aktuellt exempelvis då kommunstyrelsen har exempelvis delegerat det till vissa utpekade kommunala nämnder.

I de allmänna råden till 3 kap. 4 § tydliggörs ett antal uppgifter av strategisk betydelse för kontinuitetshanteringen och utformningen av skyddet för verksamhetsutövarens system som ledningen bör fastställa. Att verksamhetsutövaren ska fastställa riskacceptans, prioriteringsordning och sektorskritiska system, framgår av 3 kap 12 § om riskhantering, 3 kap. 14 § om kontinuitetshantering respektive 4 kap. 10 § om driftrelaterad dokumentation.

Utse roller

Kravet på att utse roller innebär inte någon skyldighet för verksamhetsutövaren att benämna roller eller ansvarsområden som det står i föreskrifterna, nämligen samordnare, informationsägare eller systemägare. Nämnda begrepp används snarast av författningstekniska skäl som ett alternativ till att skriva ”den roll eller det ansvarsområde som har i uppgift att samordna cybersäkerhetsarbetet” när en hänvisning till detta behöver göras. En roll eller motsvarande funktion behöver inte heller utgöras av en person, utan flera personer kan utgöra en roll. På samma sätt kan samma person eller funktion inneha flera roller, alternativt utgöra en del av en roll eller funktion. Så länge rollen eller funktionen finns, är det upp till verksamhetsutövaren att utforma upplägget efter sin organisation. Verksamhetsutövaren behöver dock säkerställa att det finns tillräckliga resurser för att bedriva arbetet.

Samordnare

Samordnare motsvarar närmast en informationssäkerhetssamordnare. I vissa organisationer benämns denna som CISO, det vill säga Chief Information Security Officer. Samordnaren ansvarar för att samordna cybersäkerhetarbetet hos verksamhetsutövaren. Arbetet sker som stöd för den eller de som leder cybersäkerhetsarbetet och är inte i sig en ledningsroll.

Informationsägare

Informationsägaren har ett utpekat ansvar för en viss typ eller mängd av information. Ofta sammanfaller informationsägarskapet med ansvaret i den "egna verksamheten", till exempel ansvarar en avdelningschef för den information som skapas och bearbetas av avdelningen i fråga, eller en processägare inom processen.

Det ska finnas en informationsägare för all informationsbehandling i den digitala miljön, dvs även den utkontrakterade. Av de allmänna råden till 4 kap. 4 § om förvärv av system och utkontraktering av information framgår att verksamhetsutövaren, innan utkontrakterad informationsbehandling inleds, bör kontrollera att informationsägare är utsedda för den informationshantering som utkontrakteras.

Den nivå som informationsägaren ska informera systemägaren om bedöms utifrån externa krav, interna behov och identifierade risker och med stöd av genomförd informationsklassning.

Bedömningen vad som är acceptabla tider för otillgänglighet och bristande funktionalitet för viss informationsbehandling utgår från vilka tider verksamhetsutövaren har fastslagit för den digitala miljön inom ramen för sitt kontinuitetsarbete.

Systemägare

En systemägare har ett överordnat ansvar för administration, drift och säkerhet för ett informationssystem. Systemägaren ansvarar för att informationssystemet har de tekniska säkerhetsåtgärder som behövs för att skydda informationen som hanteras där, och att det finns arbetssätt för att utvärdera och uppdatera säkerhetsåtgärder så att de ger ett tillräckligt skydd för informationssystemet.

I ansvaret för cybersäkerheten i systemet under hela dess livslängd ingår även att säkerställa att lämpliga och proportionella säkerhetsåtgärder genomförs under avvecklingen.

7.3.4 Kopplingar till andra paragrafer

Närmare om:

Ledningen

- Ledningens utbildning, 2 kap. 1 § (se avsnitt 6.1).
- Interna regler och arbetssätt, 3 kap. 3 § (se avsnitt 7.2).
- 3 kap 12 § om riskhantering (se avsnitt 7.5).
- 3 kap. 14 § om kontinuitetshantering (se avsnitt 7.6).
- 4 kap. 10 § om driftrelaterad dokumentation (se avsnitt 8.3).

Informationsägare och systemägare

- 4 kap. 4 § allmänna råd om vad som ska göras innan utkontraktering (se avsnitt 8.1).
- 3 kap. 15 § om acceptabla tider för nedsatt funktionalitet och otillgänglighet (se avsnitt 7.6).

Personalsäkerhet 3 kap. 9 §

7.3.5 Introduktion

Kontroller av personals lämplighet vid rekrytering är en viktig del av cybersäkerhetsarbetet. Genom att säkerställa att personer som ges tillgång till verksamhetens system, information och kritiska funktioner är lämpliga för sina arbetsuppgifter minskas risken för såväl avsiktliga som oavsiktliga säkerhetshot.

Brister i lämplighetsprövningen kan leda till att personer med otillräcklig kompetens eller olämpliga förutsättningar får tillgång till känsliga resurser,

vilket ökar risken för informationsläckor, otillåten påverkan, säkerhetsincidenter och verksamhetsstörningar.

7.3.6 Krav

3 kap. 9 §

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

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,
vilka kontroller som ska genomföras av personal vid förändrad åtkomst till information och system, samt
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.

7.3.7 Tolkningsstöd

Begrepp

För tolkningsstöd rörande begreppen interna regler och arbetssätt, cybersäkerhet, se Begreppslistan i inledningen.

Vilken personal som omfattas

Föreskriftskraven på kontroller och utbildning gäller såväl verksamhetsutövarens egen som inhyrd personal.

Kontroller och utbildning behöver inte se likadan ut för alla medarbetare, utan kan anpassas och utformas efter vilken roll medarbetaren har och bland annat vilken information och vilka system medarbetaren kommer få tillgång till.

Kontroll av personal

Det ställs inte krav på att verksamhetsutövaren ska genomföra kontroll mot belastningsregister. Det är upp till verksamhetsutövaren vilka kontroller som ska genomföras på vilken personal.

Utbildning, övning och övriga informationsinsatser

Föreskrifterna ställer inte något krav på att verksamhetsutövaren själv behöver anordna utbildningar och övningar. Det behöver dock säkerställas att personalen ges en sådan förståelse för verksamhetsutövarens interna regler och arbetssätt så att incidenter inte uppstår på grund av okunskap. Som nämnts i avsnittet om interna regler och arbetssätt kan dokumentation rörande i vilken utsträckning personal tagit del av exempelvis utbildning eller informationsinsatser ibland vara av betydelse för vidtagande av arbetsrättsliga åtgärder vid exempelvis allvarligare regelbrott.

Med informationsinsats avses exempelvis informationsutskick, frågestunder, information på extern webbplats eller intranät.

7.3.8 Kopplingar till andra paragrafer

Närmare om

- Ledningens utbildning 2 kap. 1 § (se avsnitt 6.1).
- Interna regler och arbetssätt 3 kap 3 § (se avsnitt 7.3).

Omvärldsbevakning 3 kap. 10 §

7.3.9 Introduktion

Omvärldsbevakning är en central del av ett effektivt cybersäkerhetsarbete. Hotbilden förändras kontinuerligt genom nya sårbarheter, angreppsmetoder och aktörer, vilket ställer krav på att organisationer löpande följer och analyserar relevanta omvärldshändelser.

Bristande omvärldsbevakning kan leda till att viktiga säkerhetsrisker inte identifieras i tid, vilket ökar sannolikheten för cyberincidenter,

verksamhetsstörningar, ekonomiska förluster samt negativ påverkan på förtroende och regelefterlevnad.

7.3.10Krav

3 kap. 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

leverantörer av den digitala miljöns hård- och mjukvara, och
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).

7.3.11Tolkningsstöd

Begrepp

För tolkningsstöd rörande begreppen cybersäkerhet och digital miljö, se Begreppslistan i inledningen.

Omvärldsbevakning

Syftet med omvärldsbevakningen är att verksamhetsutövaren ska hålla sig uppdaterad om hot, sårbarheter, teknisk utveckling, rättsliga krav och tillgängligt stöd av betydelse för verksamhetsutövarens cybersäkerhet. De källor som anges i andra stycket ska inte ses som tillräckliga för att uppnå detta syfte utan verksamhetsutövaren behöver göra en egen bedömning vilka ytterligare informationskällor som behöver bevakas för att uppnå syftet. Viss ledning ges i de allmänna råden.

Även anslutning till ANTS (Automatiska notifieringar av tekniska sårbarheter) och MISP-SE (Malware Information Sharing Platform) i enlighet med kravet i

4 kap. 20 § bidrar till omvärldsbevakning. Omvärldsbevakning kan genomföras på olika sätt, även genom deltagande i relevanta nätverk och samarbeten.

7.3.12 Kopplingar till andra paragrafer

Närmare om:

- ANTS och MISP i 4 kap. 20 § (se avsnitt 8.8).

7.4 Informationsklassning 3 kap. 11 §

7.4.1 Introduktion

Informationsklassning är en grundläggande förutsättning för ett effektivt cybersäkerhetsarbete och utgör en viktig del av organisationens systematiska och riskbaserade arbete. Genom att klassa information utifrån dess skyddsvärde får verksamhetsutövaren ett centralt ingångsvärde för bedömningen av på vilken nivå systemen behöver skyddas.

Bristande informationsklassning kan leda till felaktiga riskbedömningar, otillräckligt skydd av känslig eller verksamhetskritisk information och därmed ökad risk för obehörig åtkomst, informationsläckor, verksamhetsstörningar och bristande regelefterlevnad.

7.4.2 Krav

3 kap. 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.

7.4.3 Tolkningsstöd

Begrepp

För tolkningsstöd rörande begreppen system, cybersäkerhet, konfidentialitet, riktighet, autenticitet och tillgänglighet samt information i behov av utökat skydd, se Begreppslistan i inledningen.

Informationsklassning i relation till ”information i behov av utökat skydd”

Information i behov av utökat skydd kan i vissa fall omfattas av särskilda krav. För att veta vilken information som är i behov av utökat skydd behöver verksamhetsutövaren genomföra en informationsklassning.

Nivåer av skydd

Verksamhetsutövaren behöver anpassa nivåerna efter sin verksamhet och sina behov. Hur många nivåer och kriterier som verksamhetsutövaren behöver för sin informationsklassning kan alltså skilja sig åt. För en verksamhetsutövare kan det vara lämpligt att ha exempelvis fyra nivåer olika nivåer och kriterier för informationsklassning, medan det för en annan verksamhetsutövare kanske räcker med två nivåer eller kriterier.

Informationsklassning och system i ot-segment

Den information som styr och kontrollerar processer i ot-system och ot-segment värderas utifrån vilka konsekvenser bristande cybersäkerhet, exempelvis i form av otillgänglighet, nedsatt funktionalitet, felaktig funktion, otillåten styrning, utebliven styrning och felaktiga mät- eller larmvärden kan få för syftet med systemet och de produktionsprocesser det tillhör. Det kan exempelvis handla om konsekvenser för säkerhet, hälsa, miljö, produktion, kvalitet, leveransförmåga och viktiga samhällsfunktioner.

7.4.4 Kopplingar till andra paragrafer

Närmare om:

- Riskhantering, 3 kap. 12–13 §§ (se avsnitt 7.5).
- Kontinuitetshantering, 3 kap. 14–16 §§ (se avsnitt 7.6).
- Incidenthantering, 3 kap. 17 § (se avsnitt 7.7).

7.5 Riskhantering 3 kap. 12–13 §§

7.5.1 Introduktion

Riskhantering är en grundläggande förutsättning för ett effektivt cybersäkerhetsarbete och syftar till att identifiera, analysera, värdera och hantera risker som kan påverka verksamhetens informationstillgångar, system och tjänster. Genom ett systematiskt riskhanteringsarbete kan organisationen prioritera säkerhetsåtgärder utifrån verksamhetens behov och säkerställa att resurser används där de ger störst effekt.

Brister i riskhanteringen kan leda till att hot, sårbarheter och beroenden inte identifieras eller hanteras i tid, vilket ökar risken för säkerhetsincidenter, verksamhetsstörningar, informationsförluster och felaktiga beslut om säkerhetsåtgärder.

7.5.2 Krav

3 kap. 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.

3 kap. 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.

7.5.3 Tolkningsstöd

Begrepp

För tolkningsstöd rörande begreppen lämpliga och proportionella säkerhetsåtgärder, identifiera och hantera, utkontrakterad informationsbehandling, segment, digital miljö, se Begreppslistan i inledningen.

Att bedöma risker

Arbetet med riskbedömningar utgår från ett allriskperspektiv och syftar till att identifiera hot och sårbarheter som kan generera negativ påverkan på cybersäkerheten i verksamhetsutövarens digitala miljö. Föreskrifterna reglerar inte annan riskhantering som exempelvis tar sikte på endast ekonomiska risker för verksamhetutövaren.

Arbetet med att bedöma risker ger ett underlag för bedömningen av vilka säkerhetsåtgärder som behöver införas.

Genomförandet av riskbedömningar höjer riskmedvetenheten och ökar kunskapen inom verksamhetsutövarens organisation om hot mot och sårbarheter i organisationens digitala miljö samt vilka konsekvenser de kan få för verksamhetsutövarens organisation såväl som för samhället i stort om riskerna förverkligas.

Separata riskbedömningar

Enligt de allmänna råden bör vissa delar av verksamhetsutövarens digitala miljö bedömas separat. En riskbedömning behöver exempelvis göras för respektive segment i verksamhetsutövarens digitala miljö men också för verksamhetsutövarens samlade digitala miljö som sådan. När enskilda segment kopplas samman i en digital miljö kan riskerna samverka och förändras och i vissa fall till och med förstärkas. Detta gör att riskerna för produktionsmiljö, utvecklingsmiljö, testmiljö samt den digitala miljön i sin helhet behöver bedömas särskilt.

På samma vis ska separata bedömningar genomföras för utkontrakterad informationsbehandling och digitala leveranskedjor. Verksamhetsutövaren bör bland annat beakta sårbarheter kopplade till varje direktleverantör (leverantör som levererar sina varor och tjänster direkt till slutkunden eller

återförsäljaren) och tjänsteleverantör samt kvaliteten på leverantörernas produkter. Verksamhetsutövaren kan även behöva beakta risker som härrör från leverantörer på andra nivåer för att anses uppfylla lagens krav på säkerhetsåtgärder. Resultatet av samordnade säkerhetsriskbedömningar på unionsnivå av kritiska leveranskedjor bör beaktas. Detta syftar på de säkerhetsriskbedömningar som medlemsstaterna i samarbete med EU-kommissionen och Enisa tar fram enligt NIS2-direktivet artikel 22 rörande specifika kritiska leveranskedjor.

Det avgörs i varje enskilt fall om en verksamhetsutövare har vidtagit tillräckliga åtgärder i fråga om säkerhet i leveranskedjan, inbegripet åtgärder för att revidera avtal. Det är viktigt att verksamhetsutövaren är medveten om riskerna som följer i digitala leveranskedjor, då det är förhållanden där verksamhetsutövaren saknar fullständig kontroll över sin digitala miljö. Det har därtill blivit vanligare med incidenter i digitala leveranskedjor och denna typ av incidenter kan generera stora konsekvenser för verksamhetsutövarens digitala miljö i övrigt.

Nivåer och kriterier för bedömning av konsekvenser och sannolikhet

Konsekvenser om en risk förverkligas skulle kunna vara att en negativ samhällseffekt uppstår, merarbete för verksamhetsutövaren eller annan, ekonomisk förlust för verksamhetsutövaren eller annan, försämrad hälsa (i värsta fall dödsfall) eller ekonomiska kostnader för återställning och skadat förtroende. Vid utformandet av nivåer och kriterier för bedömning av konsekvenser behöver verksamhetsutövaren se till flera aspekter kopplat till konsekvenserna.

Dokumentation av vidtagna säkerhetsåtgärder (åtgärdsplan)

Verksamhetsutövaren ska dokumentera valda säkerhetsåtgärder och de risker som dessa säkerhetsåtgärder omhändertar i en så kallad åtgärdsplan. Föreskrifterna innebär inte några krav på att ha en enda samlad åtgärdsplan för alla delar i organisationen.

7.5.4 Kopplingar till andra paragrafer

Närmare om:

- Informationsklassning, 3 kap. 11 § (se avsnitt 7.4).
- Kontinuitetshantering, 3 kap. 14–16 §§ (se avsnitt 7.6).
- Incidenthantering, 3 kap. 17 §. (se avsnitt 7.7).
- Digitala leveranskedjor och samordnade säkerhetsbedömningar i 4 kap 2 § (se avsnitt 8.1).

7.6 Kontinuitetshantering 3 kap. 14–16 §§

7.6.1 Introduktion

Förmågan att förbereda sig för cybersäkerhetsincidenter och kriser genom kontinuitetshantering är avgörande för att upprätthålla verksamhetens funktion även vid allvarliga störningar. Genom att identifiera kritiska processer, planera för alternativa arbetssätt, fastställa återställningsförmåga och regelbundet öva hanteringen av avbrott kan organisationen minska konsekvenserna av cyberincidenter och återgå till normal verksamhet inom acceptabla tidsramar.

Brister i kontinuitetshanteringen kan leda till långvariga driftavbrott, förlorad tillgång till information och tjänster, bristande krishantering samt betydande verksamhetsmässiga, ekonomiska och samhälleliga konsekvenser vid en cyberincident eller annan allvarlig störning.

7.6.2 Krav

3 kap. 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.

3 kap. 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.

3 kap. 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.

7.6.3 Tolkningsstöd

Begrepp

För tolkningsstöd rörande begreppen cybersäkerhet, produktionsmiljö, acceptabla tider för otillgänglighet och bristande funktionalitet, utvecklings-, test-, och utbildningsmiljö, se Begreppslistan i inledningen.

Förmåga att bedriva verksamhet i händelse av inträffad incident eller kris

Kontinuitetshantering innebär att verksamhetsutövaren ska planera för och ha förmåga att upprätthålla sin verksamhet på en tolerabel nivå oavsett vilken incident eller störning den utsätts för eller om en kris inträffar. Det kan till exempel röra sig om störningar som innebär att personalen inte kan komma till arbetet, att lokalerna inte går att använda, att strömavbrott inträffar eller att leveranser av viktiga varor och tjänster inte når verksamhetsutövaren. Vilken typ av händelse som föranleder att de arbetssätt som etableras genom kontinuitetshantering behöver användas i praktiken kan variera. Styrande för bedömningen huruvida alternativa arbetssätt behöver användas eller inte beror på vilken påverkan incidenten eller krisen fått på cybersäkerheten. Incident har enligt cybersäkerhetslagen en vid betydelse, det vill säga *en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem.*

Relation till incidenthantering och krishantering

Att skapa förmåga att fungera i kriser av olika slag är ett brett arbete som kräver åtgärder i flera olika steg. Kontinuitetshantering har nära kopplingar till arbetet med incidenthantering och krishantering. Förenklat kan sägas att kontinuitetshantering handlar om att förbereda sig för att något oönskat skulle kunna ske. Incidenthanteringen stärker förmågan att hantera när något oönskat väl sker och krishanteringen tar vid då det handlar om händelser som är så stora att incidenthanteringen inte räcker till.

Prioriteringsordning för återställande av verksamhet

Föreskrifterna ställer krav på att verksamhetsutövaren fastställer en prioriteringsordning för återställning av verksamhet. Denna prioriteringsordning kan sedan ligga till grund för bedömning av vad som är acceptabla tider för nedsatt funktionalitet och otillgänglighet hos system.

Prioritering ska göras innan en incident eller kris äger rum för att säkerställa att relevant personal och funktioner i verksamheten vet hur åtgärder ska prioriteras när en incident eller kris väl inträffar.

Övning av alternativa arbetssätt

Alternativa arbetssätt bör kunna generera motsvarande funktion som ordinarie arbetssätt i största möjliga mån. Verksamhetsutövaren ska öva de alternativa arbetssätt som tagits fram. Detta för att utbilda personalen och främja att verksamheten kan fortgå så effektivt som möjligt då dessa arbetssätt behöver nyttjas till följd av en incident eller kris.

Övningar kan genomföras dels inom verksamhetsutövarens organisation, men verksamhetsutövaren kan också genomföra övningar med externa parter. Exempelvis kan kommuner, när de finner de lämpligt genomföra gemensamma övningar.

Förtydligande av roller, ansvarsområden och befogenheter

För att en verksamhet ska kunna fungera vid incidenter eller kriser av olika slag är det viktigt att det står klart vem som ska göra vad och vem som kan fatta vilka beslut. Detta ska finnas på plats för att skapa en handlingskraftig verksamhet som kan agera effektivt i kris av olika slag. De roller och funktioner som redan finns utpekade (samordnare, systemägare och informationsägare) skulle kunna vara exempel på sådana roller som skulle kunna få utökat mandat vid en incident eller kris. Det bör dock vara tydligt när sådana extra roller eller befogenheter träder in. Det är upp till verksamhetsutövaren att göra denna bedömning för sin verksamhet.

7.6.4 Kopplingar till andra paragrafer

Närmare om:

- Incidenthantering 3 kap. 17 § (se avsnitt 7.7).
- Krishantering 3 kap 18 § (se avsnitt 7.8).

7.7 Incidenthantering 3 kap. 17 §

7.7.1 Introduktion

Incidenthantering är en central del av cybersäkerhetsarbetet och syftar till att säkerställa att säkerhetsincidenter upptäcks, rapporteras, analyseras, hanteras och följs upp på ett strukturerat och effektivt sätt. Genom etablerade processer, tydliga ansvarsförhållanden och förberedda åtgärder kan organisationen begränsa konsekvenserna av incidenter, återställa normal verksamhet och stärka sin motståndskraft över tid.

Brister i incidenthanteringen kan leda till fördröjd upptäckt, otillräckliga åtgärder och förlängda störningar, vilket ökar risken för informationsläckor, verksamhetsavbrott, större skador på system och information samt minskat förtroende för verksamheten.

7.7.2 Krav

3 kap. 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.

7.7.3 Tolkningsstöd

Begrepp

För tolkningsstöd rörande begreppen cybersäkerhet, produktionsmiljö, acceptabla tider för otillgänglighet och bristande funktionalitet, utvecklings-, test-, och utbildningsmiljö, se Begreppslistan i inledningen.

Incidenter och tillbud

Vad som utgör en incident definieras i cybersäkerhetslagens 1 kap. 2 § 10 p som *en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem*. Händelser som inte når upp till tröskeln för att utgöra en incident i cybersäkerhetslagens mening kallas i föreskrifterna ”tillbud”. Tillbud inkluderar mindre avvikelser som sammantaget indikerar på problematik.

Incidenthantering

Incidenthantering avser alla åtgärder och förfaranden som syftar till att förebygga, upptäcka, analysera, begränsa eller reagera på och återhämta sig från en incident. Verksamhetsutövaren ska säkerställa att incidenter och tillbud kan upptäckas och anmälas i enlighet med externa krav på incidentrapportering men även att incidenten eller tillbudet anmäls till rätt roll eller funktion inom verksamhetsutövarens egen organisation. Därefter behöver incidenten eller tillbudet analyseras eller hanteras. Förmåga att göra detta kan finnas hos verksamhetsutövarens egen personal, eller omhändertas av inhyrd personal såsom exempelvis konsultbolag.

Med extern rapportering av incidenter syftas inte endast på sådan incidentrapportering som ska ske enligt cybersäkerhetslagen utan även enligt exempelvis andra regelverk såsom dataskyddsförordningen, säkerhetsskyddslagen eller branschspecifika regler.

Efter en incident eller ett tillbud ska verksamhetsutövaren arbeta med återställande av information samt vidta förebyggande åtgärder för att förhindra att liknande incidenter sker i den digitala miljön. Om det är oklart vad som orsakade incidenten eller tillbudet och detta utgör ett hinder för att vidta lämpliga åtgärder finns sannolikt anledning att utreda incidentens grundorsak.

7.7.4 Kopplingar till andra paragrafer

Närmare om:

- Kontinuitetshantering 3 kap. 14–16 §§ (se avsnitt 7.6).
- Krishantering 3 kap 18 § (se avsnitt 7.8).

7.8 Krishantering 3 kap. 18 §

7.8.1 Introduktion

Krishantering är en viktig del av cybersäkerhetsarbetet för att kunna hantera säkerhetsincidenter som är så omfattande, komplexa eller allvarliga att de inte kan omhändertas inom ramen för den ordinarie incidenthanteringen. Genom

etablerade krisledningsstrukturer, tydliga beslutsvägar, samordning och kommunikationsrutiner kan organisationen hantera extraordinära händelser som riskerar att få betydande konsekvenser för verksamheten, samhällsviktiga tjänster eller förtroendet för organisationen.

Brister i krishanteringen kan leda till fördröjda beslut, bristande samordning, otillräcklig kommunikation och en försvagad förmåga att hantera allvarliga säkerhetshändelser, vilket kan medföra omfattande verksamhetsstörningar, ökade skador och förlängd återhämtningstid.

7.8.2 Krav

3 kap. 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.

7.8.3 Tolkningsstöd

Begrepp

För tolkningsstöd rörande begreppen cybersäkerhet, produktionsmiljö, acceptabla tider för otillgänglighet och bristande funktionalitet, utvecklings-, test-, och utbildningsmiljö, se Begreppslistan i inledningen.

När aktualiseras krishanteringen

Det går inte att på förhand säga vilka inträffade incidenter som är att beakta som en kris som i sin tur aktualiserar verksamhetsutövarens krishantering. Verksamhetsutövaren kan utgå från två kriterier:

1. händelsen ska påverka cybersäkerheten, och
2. händelsen ska inte kunna hanteras inom ramen för ordinarie incidenthantering.

Utifrån dessa kriterier är det upp till verksamhetsutövaren att avgöra när krishantering inom organisationen blir aktuell.

Händelser som aktualiserar en verksamhetsutövarens krishantering kan exempelvis vara sådana som innebär att personalen inte kan komma till arbetet, att lokalerna inte går att använda, att strömavbrott inträffar eller att leveranser av viktiga varor och tjänster inte når verksamhetsutövaren.

Förhållandet till övriga krisfunktioner i verksamhetsutövarens organisation

Vissa organisationer kanske redan har en etablerad stabsmetodik med rutiner för hur organisationer agerar vid olika typer av kriser. Det som avses med ”etablerat” stabsmetodik i föreskriftens allmänna råd är alltså sådan struktur som verksamhetsutövaren redan har, alternativt sådan som verksamhetsutövaren etablerat i enlighet med 3 kap. 16 § i föreskrifterna.

Syftet med att ha en etablerad stabsmetodik och struktur är att säkerställa förmåga att kunna arbeta på ett ändamålsenligt sätt med krisen. Det kan exempelvis handla om att korta ned beslutsflöden, prioritera och samla resurser.

I likhet med kontinuitetshantering kan verksamhetsutövare öva sin krishantering antingen inom organisationen, eller där verksamhetsutövaren bedömer det lämpligt, tillsammans med andra organisationer. Vid övning tillsammans med andra organisationer kan bland annat kriskommunikationen övas.

7.8.4 Kopplingar till andra paragrafer

Närmare om:

- Kontinuitetshantering 3 kap. 14–16 §§ (se avsnitt 7.6).
- Krisorganisation 3 kap. 16 § (se avsnitt 7.6).
- Incidenthantering 3 kap 17 § (se avsnitt 7.7).

7.9 Uppföljning och utvärdering 3 kap. 19 §

7.9.1 Introduktion

Uppföljning och utvärdering är viktiga förutsättningar för att säkerställa att cybersäkerhetsarbetet är effektivt, ändamålsenligt och anpassat till verksamhetens risker och behov. Genom regelbunden uppföljning av säkerhetsåtgärder, processer och incidenter kan organisationen identifiera brister, mäta effekten av vidtagna åtgärder och kontinuerligt förbättra sin säkerhetsförmåga.

Brister i uppföljning och utvärdering kan leda till att säkerhetsproblem, sårbarheter och avvikelser förblir oupptäckta, att ineffektiva säkerhetsåtgärder kvarstår samt att organisationens förmåga att förebygga, upptäcka och hantera cyberhot successivt försämras.

7.9.2 Krav

3 kap. 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.

7.9.3 Tolkningsstöd

Begrepp

För tolkningsstöd rörande begreppen externa krav, interna behov och identifierade risker, digital miljö och sektorskritiska system, se Begreppslistan i inledningen.

Uppföljning och utvärdering

Uppföljning och utvärdering av cybersäkerhetsarbetet och säkerhetsåtgärder är en central del i ett systematiskt och riskbaserat cybersäkerhetsarbete. Detta gäller särskilt i en föränderlig miljö.

Med uppföljning avses mer av en löpande och rutinmässig kontroll som dokumenterar vad som händer under ett pågående arbete för att se om arbetet följer planen. Utvärdering utgörs mer av en systematisk undersökning och bedömning av värdet, resultatet eller kvaliteten på ett arbete exempelvis mot satta mål. Gränsen mellan uppföljning och utvärdering är inte tydlig utan de kompletterar varandra.

Resultatet från uppföljning och utvärdering utgör underlag för ledningens arbete med att godkänna och övervaka cybersäkerhetsarbetet.

7.9.4 Kopplingar till andra paragrafer

Närmare om:

- Systematiskt och riskbaserat arbete 3 kap. 1–2 §§ (se avsnitt 7.1).
- Roller, ansvarsområden och befogenheter 3 kap. 4 – 8 §§ (se avsnitt 7.3).

8 Fjärde kapitlet Tekniska och driftrelaterade säkerhetsåtgärder

8.1 Förvärv av system och utkontraktering av informationsbehandling 4 kap. 1 – 4 §§

8.1.1 Introduktion

God kravställning med tydliga säkerhetskrav är en viktig förutsättning för att upprätthålla cybersäkerhet i den egna organisationen och i digitala leveranskedjor. Genom att ställa krav på leverantörer, produkter, tjänster och externa parter kan organisationen säkerställa att säkerhetsrisker identifieras och hanteras genom hela livscykeln samt att beroenden till externa aktörer inte medför oacceptabla risker.

Brister i kravställningen kan leda till att sårbarheter, säkerhetsbrister eller otillräckliga skyddsåtgärder byggs in i verksamhetens system och tjänster, vilket ökar risken för cyberangrepp, informationsläckor, leveransstörningar och andra incidenter som kan få betydande konsekvenser för verksamheten.

8.1.2 Krav

4 kap. 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.

4 kap. 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.

4 kap. 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.

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 kap. 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, informations-ägare är utsedda för den informationshantering som utkontrakteras, och tilltänkt leverantör uppfyller ställda krav på säkerhetsåtgärder.

8.1.3 Tolkningsstöd

Begrepp och formuleringar

För tolkningsstöd rörande begreppen och formuleringarna utkontraktering av informationsbehandling, identifiera och hantera, leverantör, informationsägare och systemägare, lämpliga och proportionerliga säkerhetsåtgärder samt intern verksamhet och externa tjänster, se Begreppslistan i inledningen.

Utkontraktering och kravuppfyllnad

I det fall som verksamhetsutövaren förvärvar hela eller delar av system eller utkontrakterar hela eller delar av sin informationsbehandling ska verksamhetsutövaren säkerställa att krav på säkerhetsåtgärder som är tillämpliga vid förvärv eller utkontraktering ställs på vald leverantör. Det handlar om krav i föreskrifterna som verksamhetsutövaren själv skulle ha

behövt uppfylla på cybersäkerhet om verksamhetsutövaren inte anlitat en leverantör, exempelvis på säkerhetstester, driftdokumentation och incidenthantering.

Kraven på cybersäkerhet gäller endast de leverantörer som verksamhetsutövaren utkontrakterat informationsbehandling till eller förvärvat system från. I det allmänna rådet ges exempel på ett antal säkerhetsåtgärder som bör inkluderas i avtal eller överenskommelse med leverantören. Vilka säkerhetsåtgärder som ska inkluderas i respektive avtal utgår från verksamhetsutövarens bedömning av risk, informationsklassning samt verksamhetens syfte och organisation. Listan är alltså inte uttömmande, och verksamhetsutövaren kan utifrån ovan nämnd bedömning inkludera ytterligare krav.

Leverans av tekniska försörjningssystem såsom el, värme, elektronisk kommunikation mm regleras närmare i 4 § kapitel 5. Precis som med övriga säkerhetskrav behöver en verksamhetsutövare själv uppfylla dessa krav för att skydda sina system – vid exempelvis utkontraktering av informationsbehandling behöver de även uppfyllas av leverantören.

Närmare om avtal

Verksamhetsutövaren behöver identifiera vilka avtal som inte ställer tillräckliga cybersäkerhetskrav och sedan göra en bedömning av hur eventuella brister ska hanteras. Det är dock inte alltid ekonomiskt försvarbart att omförhandla ett avtal under pågående avtalsperiod. I så fall får man vidta andra åtgärder för att omhänderta identifierade risker - exempelvis kan det handla om en egen extra kontroll av levererad programvara för att säkerställa att den inte innehåller någon skadlig kod innan den installeras.

Kravet på att utvärdera om verksamhetsutövaren kan uppfylla ställda krav på cybersäkerhet kan uppfyllas med stöd av olika information såsom om kunskap och kompetens, storlek, tidigare erfarenheter och liknande.

När det gäller krav på om leverantören kan uppfylla sina åtaganden kan detta exempelvis ske genom att ställa krav på cybersäkerhetskompetens hos leverantören, att leverantören genomför kontroller av hård- och mjukvara med mera.

Leveranskedjor

Kontinuitet i leveranskedjorna kan exempelvis handla om att så långt möjligt undvika kritiska beroenden, det vill säga att organisationen är helt beroende av en enda leverantör.

Om den specifika komponenten slutar tillverkas eller om leverantören slås ut av ett cyberangrepp eller går i konkurs, riskerar hela verksamheten att lamslås om det saknas redundans eller alternativa lösningar. Här behöver verksamhetsutövaren se över möjligheterna att bygga upp redundans.

Med relevant information om underleverantörer avses sådan information som verksamhetsutövaren behöver för att exempelvis identifiera monoberoenden eller svaga underleverantörer. Utöver namn och organisationsnummer kan det vara information om leverantörens överväganden när underleverantören anlitades. Behovet av sådan information kan exempelvis hanteras genom att skrivas in i avtalet med leverantören eller begäras in i samband med urvalsprocessen vid utkontraktering av informationsbehandling eller förvärv av system.

Resultatet av de samordnade säkerhetsriskbedömningar av kritiska leveranskedjor som utförs i enlighet med artikel 22.1 i NIS 2-direktivet kan innebära att vissa typer av produkter eller tjänster inte längre får importeras till eller användas i EU. Artikel 22.1 ger NIS Samarbetsgruppen, i samarbete med ENISA och kommissionen, rätt att utföra samordnade säkerhetsriskbedömningar av specifika kritiska leveranskedjor för IKT-tjänster, IKT-system eller IKT-produkter. De samordnade säkerhetsriskbedömningar, exempelvis IKT-verktygslådan, finns att läsa här: https://digital-strategy.ec.europa.eu/en/library/toolbox-improve-ict-supply-chain-security.

8.1.4 Kopplingar till andra paragrafer

Närmare om:

- Informationsklassning i 3 kap. 11 § (se avsnitt 7.4).
- Riskhantering i 3 kap. 12–13 §§ (se avsnitt 7.5).
- Kontinuitetshantering i 3 kap. 14 § (se avsnitt 7.6).
- Krav på tekniska försörjningssystem finns i 4 kap 5 § (se avsnitt 8.2).

8.2 Utveckling, underhåll och avveckling av system 4 kap. 5 – 7 §§

8.2.1 Introduktion

Cybersäkerhet vid utveckling, underhåll och avveckling av system är avgörande för att säkerställa att säkerhetskrav beaktas under hela systemets livscykel. Genom att integrera säkerhet i utvecklingsprocesser, genomföra säkert underhåll och hantera avveckling på ett kontrollerat sätt kan organisationen minska risken för sårbarheter, felaktiga konfigurationer, kvarvarande data och andra säkerhetsbrister.

Brister i hanteringen av systemens livscykel kan leda till att sårbarheter byggs in i eller kvarstår i system, att känslig information exponeras vid förändringar eller avveckling samt att föråldrade och osäkra system fortsätter att användas, vilket ökar risken för cyberangrepp, informationsläckor och verksamhetsstörningar.

8.2.2 Krav

4 kap. 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.

4 kap. 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.

4 kap. 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.

8.2.3 Tolkningsstöd

Begrepp

För tolkningsstöd rörande begreppen informationsägare, systemägare, digital miljö, lämpliga och proportionerliga säkerhetsåtgärder se begreppslistan.

Säker utveckling

Med säker utveckling avses att arbeta strukturerat med cybersäkerhet från tidiga krav till att systemet är färdigt. Arbetssättet är väletablerat och det finns en rad stöd att tillgå.

Dokumentation och resurser

Ledning för vad som ingår i nödvändig dokumentation för drift och förvaltning hämtas i 4 kap. 8 – 10 §§.

Beslut om att påbörja informationsbehandling

Det är vanligt att informationsägaren fattar beslut om att påbörja informationsbehandling i ett system men verksamhetsutövaren kan välja en annan mandatfördelning om det passar den egna beslutsstrukturen bättre.

8.2.4 Kopplingar till andra paragrafer

Närmare om:

- informationsägarens uppgifter 3 kap. 7 § (se avsnitt 7.3).
- systemägarens uppgifter 3 kap. 8 § (se avsnitt 7.3).
- informationsklassning 3 kap. 11 § (se avsnitt 7.4).
- riskanalys 3 kap. 12 § (se avsnitt 7.5).
- åtgärdsplan 3 kap. 13 § (se avsnitt 7.5).
- säkerhetstester och granskningar 4 kap. 27 § (se avsnitt 8.12).
- ledningens resurstilldelning 3 kap. 4 § (se avsnitt 7.4).
- ändringshantering och säker utveckling 4 kap. 30 och 31 §§ (se avsnitt 8.15).

8.3 Driftrelaterad dokumentation 4 kap. 8–10 §§

8.3.1 Introduktion

Aktuell och ändamålsenlig dokumentation över den digitala miljön, dess system, beroenden och driftprocesser är en viktig förutsättning för ett effektivt cybersäkerhetsarbete. Dokumentationen ger stöd för riskanalyser,

incidenthantering, förändringsarbete och kontinuitetsplanering genom att skapa förståelse för vilka tillgångar som finns och hur de samverkar.

Bristande eller inaktuell dokumentation kan leda till att sårbarheter, kritiska beroenden och risker inte identifieras, vilket ökar risken för säkerhetsincidenter, driftstörningar, förlängda återställningstider och felaktiga riskbedömningar.

8.3.2 Krav

4 kap. 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.

4 kap. 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.

4 kap. 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.

8.3.3 Tolkningsstöd

Begrepp

För tolkningsstöd rörande begreppen skyndsamt, digital miljö, produktions-, utvecklings-, test- och utbildningsmiljö, utkontrakterad informationsbehandling, informationsägare, systemägare, sektorskritiska system, intern verksamhet och externa tjänster, viktiga samhällsfunktioner, it- och ot-segment, information i behov av utökat skydd, se begreppslistan.

Dokumentation

Dokumentation sker på tre olika nivåer - arkitekturen över den digitala miljön, förteckningen respektive driftdokumentation. Syftet med förteckningen är att ha en enkelt tillgänglig information som kan användas vid exempelvis incidenter för att snabbt hitta och förmedla den ur ett hanteringsperspektiv mest relevanta informationen.

Verksamhetsutövaren avgör själv exakt vad som ska dokumenteras och hur detaljerad dokumentationen ska vara. Bedömningen görs utifrån genomförd riskanalys.

8.3.4 Kopplingar till andra paragrafer

Närmare om:

- Indelning i segment 4 kap. 11 – 12 §§ (se avsnitt 8.4).
- Konfigurering av informationsflöden 4 kap 13 § (se avsnitt 8.5).
- Acceptabla tider för otillgänglighet och bristande funktionalitet 3 kap. 15 § (se avsnitt 7.6).
- Återställning av förlorad information och säkerhetskopiering 4 kap. 28 § (se avsnitt 8.13).

8.4 Segmentering 11–12 §§

8.4.1 Introduktion

Genom att dela upp den digitala miljön i segment och begränsa dataflöden utifrån verksamhetens behov kan konsekvenserna av sårbarheter och säkerhetsincidenter minskas.

Bristande segmentering och otillräcklig kontroll av informationsflöden ökar risken för att angrepp, skadlig kod eller obehörig åtkomst sprids mellan system, vilket kan leda till omfattande verksamhetsstörningar, informationsläckor och ökad påverkan vid incidenter.

8.4.2 Krav

4 kap. 11 §

För att minimera konsekvenser och förhindra spridning av incidenter orsakade av angrepp mot och misstag i den digitala miljön ska verksamhetsutövaren dela in den i segment och endast tillåta godkända informationsflöden 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.

4 kap. 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.

8.4.3 Tolkningsstöd

Begrepp

För tolkningsstöd rörande begreppen digital miljö, system, produktions-, utvecklings-, test- och utbildningsmiljö, sektorskritiska system, externa tjänster, viktiga samhällsfunktioner, segment, it- och ot-segment, se begreppslistan.

Godkända informationsflöden

Med godkända informationsflöden avses i föreskrifterna sådana informationsflöden som verksamhetsutövaren aktivt tagit ställning till och godkänt förekomsten av. Utgångspunkten när verksamhetsutövaren ska bedöma om ett visst informationsflöde mellan segment ska tillåtas eller inte är risken för konsekvenser och spridning av incidenter i den digitala miljön. Olika informationsflöden kan godkännas mellan olika segment beroende på vilka system som är placerade i de olika segmenten. Till och från ett segment med system som används för externa tjänster behöver sannolikt fler och andra informationsflöden godkännas än till och från ett segment med system som innehåller sårbarheter som inte kan omhändertas på ett tillfredställande sätt.

Det är lämpligt att utgå från en riskbedömning vid bedömningen av vilka informationsflöden som ska godkännas. Eftersom segmentering och säkerhetskonfigurering är två säkerhetsåtgärder med nära koppling och som är ömsesidigt förstärkande är det även lämpligt att arbeta samlat med dessa uppgifter. Föreskrifterna innehåller inte några krav på vem som ska godkänna informationsflödena, det tydliggör verksamhetsutövaren lämpligen i sina interna regler och arbetssätt rörande segmentering.

It- och ot-segment

Verksamhetsutövaren ska placera system i antingen it-segment eller ot-segment. En övergripande skillnad mellan it- och ot-segment är att det i ot-segment finns möjlighet att vidta vissa säkerhetsåtgärder på segmentnivå i stället för på systemnivå. Någon skillnad i nivån av säkerhet avses inte utan det handlar främst om ett alternativt sätt att lösa säkerhetsbehovet. I ot-segment placeras sådana ot-system, ibland även kallade cyberfysiska system som, exempelvis på grund av hög risk för allvarliga driftstörningar, inte är lämpliga att skydda på systemnivå. Det finns många ot-system som är väl anpassade för att skyddas på samma sätt som it-system som används i exempelvis kontorsmiljö.

Exempelvis: Ett äldre system som används för att styra ett vattenkraftverk är kanske inte möjligt att uppdatera utan driftstörningar med konsekvenser för elproduktionen. Detta system placeras med fördel i ett ot-segment där säkerhetsåtgärder vidtas på segmentnivå som omhändertar de risker som avsaknad av frekventa uppdatering medför.

Inrätta utvecklings-, test- och utbildningsmiljö

Särskilda miljöer för utveckling, test och utbildning ska inrättas när det föreligger risk att sådan verksamhet påverkar cybersäkerheten i produktionsmiljöns it-segment. Det är med andra ord inte något krav på att alltid inrätta den här typen av miljöer. I det fall exempelvis utbildning för de egna användarna kan bedrivas utan någon risk för cybersäkerheten i

produktionsmiljön uppstår går det utmärkt att verksamhetsutövarens digitala miljö enbart består av produktionsmiljö.

Det finns inte några hinder för verksamhetsutövaren att inrätta en eller flera olika produktions-, utvecklings-, test- och utbildningsmiljöer. Det centrala är att välja vilken typ av miljö det handlar om. Det är även möjligt att ha en kombinerad utvecklings-, test- och utbildningsmiljö - det är dock lämpligt i sådana fall att identifiera om några särskilda risker uppkommer genom att göra en sådan kombination. Eventuella risker omhändertas lämpligen inom ramen för verksamhetsutövarens riskhantering.

Verksamhetsutövaren ska identifiera och hantera motsvarande behov för ot-segment. Det är med andra ord inte ett ”ska-krav” även om det påverkar cybersäkerheten i produktionsmiljön.

8.4.4 Kopplingar till andra paragrafer

Närmare om

- Interna regler och arbetssätt 3 kap. 3 § (se avsnitt 7.2).
- Riskhantering 3 kap. 12 – 13 §§ (se avsnitt 7.5).
- Säkerhetskonfigurering 4 kap. 13 § (se avsnitt 8.5).

8.5 Säkerhetskonfigurering 4 kap. 13 §

8.5.1 Introduktion

Säkerhetskonfigurering är en grundläggande förutsättning för att skydda system, nätverk och information mot cyberhot. Genom att konfigurera system enligt etablerade säkerhetskrav, exempelvis genom att begränsa funktioner, stänga onödiga tjänster och tillämpa säkra standardinställningar, minskas antalet sårbarheter och angreppsvägar.

Brister i säkerhetskonfigureringen kan leda till att system exponeras för onödiga risker, vilket ökar sannolikheten för obehörig åtkomst, säkerhetsincidenter, informationsläckor och driftstörningar.

8.5.2 Krav

4 kap. 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.

8.5.3 Tolkningsstöd

Begrepp

För tolkningsstöd rörande begreppen system, cybersäkerhet och klienter, se begreppslistan.

Godkända informationsflöden

Läs mer om godkända informationsflöden i avsnitt 8.4.3.

Förinställda autentiseringsuppgifter, funktioner i system som inte behövs

Med förinställda autentiseringsuppgifter syftas på de standardinställningarna

som medföljer från tillverkaren vid förvärv av exempelvis mjukvara.

Funktioner i system som inte behövs, är sådana system eller funktioner i system som inte behövs vara tillgängliga i den digitala miljön för att upprätthålla verksamheten. Att helt inaktivera den onödiga funktionen eller att eliminera funktionen från åtkomst kan minska risken.

På förhand godkänd mjukvara

Formuleringen syftar på så kallad vitlistning där verksamhetsutövaren endast tillåter att av verksamhetsutövaren på förhand godkänd mjukvara installeras i den digitala miljön.

Direktkommunikation mellan klienter

Kommunikation mellan exempelvis användarklienter sker vanligtvis via en central funktion, något som underlättar exempelvis arbetet med att skydda mot skadlig kod. I de allmänna råden rekommenderas att direktkommunikation inte tillåts eftersom det försvårar cybersäkerhetsarbetet.

Fördefinierad tidsperiod

Vilken den fördefinierade tidsperioden är bestäms av verksamhetsutövaren. Den framgår lämpligtvis av interna regler och arbetssätt.

Att upprätthålla säkerhet

För att säkerställa att exempelvis brandväggar och andra säkerhetsfunktioner inte öppnas upp vid exempelvis strömavbrott (fail-safe) rekommenderas i de allmänna råden att säkerhetsfunktioner konfigureras så att säkerhet upprätthålls när tekniska fel och brister inträffar.

8.5.4 Kopplingar till andra paragrafer

Närmare om:

- Segmentering och godkända informationsflöden 4 kap. 11 – 12 §§ (se avsnitt 8.4).
- Behörighetshantering och autentiseringsuppgifter 4 kap. 14 § (se avsnitt 8.6).
- Interna regler och arbetssätt 3 kap. 3 § (se avsnitt 7.2).

8.6 Behörighetshantering och autentisering 4 kap. 14 – 19 §§

8.6.1 Introduktion

Behörighetshantering och autentisering är grundläggande säkerhetsåtgärder för att säkerställa att endast behöriga användare får tillgång till system, information och funktioner utifrån sina arbetsuppgifter. Genom tydliga behörighetsprinciper och stark autentisering minskas risken för obehörig åtkomst och felaktig användning av verksamhetens informationsresurser.

Brister i behörighetshantering eller autentisering kan leda till att användare får för omfattande åtkomster eller att obehöriga kan få tillgång till känslig information, vilket ökar risken för informationsläckor, manipulation av data, säkerhetsincidenter och verksamhetsstörningar.

8.6.2 Krav

4 kap. 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.

4 kap. 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.

4 kap. 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.

4 kap. 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.

4 kap. 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.

4 kap. 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.

8.6.3 Tolkningsstöd

Begrepp

För tolkningsstöd rörande begreppen digital miljö, information i behov av utökat skydd, identifiera och hantera, system, se begreppslistan.

Digitala identiteter, behörigheter och autentiseringsuppgifter

En person eller ett system ges en digital identitet för att kunna agera i den digitala miljön, denna digitala identitet kan ha flera behörigheter beroende på vad personen eller systemet är tänkt att göra. Systembehörighet ska tilldelas restriktivt eftersom det ger den digitala identiteten stor möjlighet att påverka den digitala miljön. Autentiseringsuppgifter är de uppgifter som behövs för att få tillgång till den digitala identiteten och behörigheten, exempelvis användarnamn och lösenord.

Vad som är tillräcklig längd och komplexitet hos autentiseringsuppgifter behöver bestämmas utifrån identifierade risker och användningsområde.

Tillgång till digital den miljön

Behörigheter kan avse större eller mindre delar av den digitala miljön. Föreskrifterna utgör inte något hinder mot att ge allmänheten tillgång till vissa delar av den digitala miljön, exempelvis en eller flera av verksamhetsutövarens externa tjänster.

Externa tjänster som är avsedda att användas av allmänheten eller annan extern grupp ska enligt 4 kap. 11 § avgränsas från övriga delar av den digitala miljön genom segmentering för att säkerställa att dessa delar inte blir åtkomliga för obehöriga.

Kravet i 4 kap. 17 § innebär ett krav på flerfaktorsautentisering när personal och leverantörer ges tillträde till den digitala miljön via externt nätverk, exempelvis vid distansarbete.

Möjlighet att verifiera användares respektive verksamhetsutövares identitet

Antalet tillgängliga tjänster på nätet ökar och med det även risken för bedrägerier där förövaren antingen utger sig för att vara en användare eller exempelvis en bank, vårdinrättning eller annan aktör som den drabbade önskar kontakt med. Den ökade risken för brottslighet på nätet utgör bakgrunden för kravet i 4 kap. 18 § av att bedöma behovet av att införa krav på e-legitimation för användare av verksamhetsutövarens tjänster respektive kravet i 4 kap. 19 § av att bedöma behovet av att ge andra möjlighet att verifiera verksamhetsutövarens identitet vid kontakt via digitala kanaler.

Låsning av konton

Det är upp till verksamhetsutövaren att fastställa hur många misslyckade inloggningsförsök som föranleder att den digitala identiteten låser sig. Bedömningen bör göras utifrån externa krav, interna behov och identifierade risker.

8.6.4 Kopplingar till andra paragrafer

Närmare om:

- Segmentering 4 kap. 11 – 12 §§ (se avsnitt 8.4).
- Säkerhetskonfigurering 4 kap. 13 § (se avsnitt 8.5).
- Intrångsdetektering och intrångsskydd 4 kap. 29 § (se avsnitt 8.14).

8.7 Övervakning, säkerhetsloggning och logganalys 4 kap. 20 – 22 §§

8.7.1 Introduktion

Övervakning av system, säkerhetsloggning och logganalys är viktiga förutsättningar för att upptäcka, utreda och hantera säkerhetshändelser i den digitala miljön. Genom att samla in och analysera loggar kan avvikelser, misstänkta aktiviteter och pågående angrepp identifieras i ett tidigt skede, vilket möjliggör snabba och effektiva åtgärder.

Brister i övervakning, loggning eller logganalys kan leda till att säkerhetsincidenter förblir oupptäckta eller upptäcks för sent, vilket ökar risken för informationsläckor, verksamhetsstörningar, försvårad incidentutredning och större konsekvenser vid angrepp.

8.7.2 Krav

4 kap. 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 realtidsövervakning i den digitala miljön.

Allmänna råd

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

4 kap. 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.

4 kap. 22 §

Verksamhetsutövaren ska analysera säkerhetsloggarna för att upptäcka och utreda fel, obehörig åtkomst och andra brister i cyber säkerheten.

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.

8.7.3 Tolkningsstöd

Begrepp

För tolkningsstöd rörande begreppen cybersäkerhet, identifiera och hantera behovet av, produktionsmiljö, digital miljö, realtidsövervakning, information i behov av utökat skydd, sektorskritiska system, segment, utvecklings-, test- och utbildningsmiljö, se begreppslistan.

ANTS och MISP

Automatiska notifieringar av tekniska sårbarheter (ANTS) är en kostnadsfri tjänst som tillhandahålls av den nationella CSIRT-enheten hos nationellt cybersäkerhetscenter (NCSC). ANTS ger verksamhetsutövaren stöd för att övervaka sina angreppsytor på internet. Syftet är att snabbt notifiera organisationer när det identifierats företeelser som kan behöva åtgärdas i deras tillgångar på internet, exempelvis sårbarheter som kan nyttjas i antagonistiskt syfte. Föreskrifterna innebär ett krav på anslutning såvida det inte bedöms som uppenbart obehövligt. Vad som är att anse som uppenbart obehövligt bedöms från fall till fall. Det är en hög tröskel men skulle eventuellt kunna bestå i att en organisation redan har en sådan funktionalitet som fullt ut och över tid tillhandahåller minst samma funktionalitet och stöd som erbjuds av NCSC via ANTS.

Malware Information Sharing Platform (MISP) är en plattform för informationsdelning om cyberhot och it-incidenter som lanserats av NCSC. Genom MISP-SE kan organisationer dela, och ta del av andras, cyberhotinformation vilket bidrar till snabbare upptäckt av cyberangrepp och ett starkare gemensamt skydd. Syftet är att stärka Sveriges samlade motståndskraft mot cyberangrepp. Eftersom det finns ett antal krav som en verksamhetsutövare behöver uppfylla innan anslutning till MISP är kravet i 4 kap. 20 § 3 inte absolut utan formulerat som att anslutning ska ske – om möjligt. Formuleringen tar sikte på de situationer där verksamhetsutövaren inte uppfyller anslutningsvillkoren i MISP.

ANTS och MISP bidrar även till omvärldsbevakning.

8.7.4 Kopplingar till andra paragrafer

Närmare om:

- Omvärldsbevakning 3 kap. 10 § (se avsnitt 7.3).
- Incidenthantering 3 kap. 17 § (se avsnitt 7.7).
- Krishantering 3 kap. 18 § (se avsnitt 7.8).
- Segmentering 4 kap. 11 § (se avsnitt 8.4).
- Robust och korrekt tid 4 kap. 23 § (se avsnitt 8.9).

8.8 Robust och korrekt tid 4 kap. 23 §

8.8.1 Introduktion

Tillgång till robust och korrekt tid är en viktig förutsättning för ett effektivt cybersäkerhetsarbete. Synkroniserad tid mellan system möjliggör korrekt loggning, övervakning, händelseanalys och incidentutredning samt stödjer säkerhetsfunktioner som autentisering och kryptering.

Brister i tidssynkronisering eller tillförlitlig tidskälla kan leda till felaktiga loggar, försvårad spårbarhet och minskad förmåga att upptäcka, analysera och hantera säkerhetsincidenter, vilket ökar risken för verksamhetsstörningar och säkerhetsrelaterade fel.

8.8.2 Krav

4 kap. 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.

8.8.3 Tolkningsstöd

Begrepp och formuleringar

För tolkningsstöd rörande begreppen utvecklings-, test- och utbildningsmiljö, se begreppslistan.

Översättningsbar till UTC (SP)

UTC (SP) utgör grunden för den officiella tid som används i Sverige. Den upprätthålls och distribueras av RISE (Research Institutes of Sweden) via riksmätplatsen i Borås. Tidsskalan baseras på fem atomklockor i Borås som mäter sekunden dygnet runt och synkroniseras med det internationella UTC-medelvärdet (från BIPM i Paris). Kravet i föreskrifterna på att verksamhetsutövaren ska använda robust och korrekt tid som är översättningsbar till UTC (SP) hindrar inte att en annan tid används (exempelvis en koncerngemensam tid) däremot ska den använda tiden vid behov kunna uttryckas i UTC (SP) tid.

UTC(SP) är en mycket exakt tid och sekunderna mäts kontinuerligt. På vilken detaljnivå som verksamhetsutövare synkroniserar med eller översätter sin tid till UTC(SP) beror på verksamheten och syftet. Ett övergripande syfte är att kunna jämföra säkerhetsloggar både internt och externt.

8.8.4 Kopplingar till andra paragrafer

Närmare om:

- Säkerhetsloggning och logganalys 4. kap. 21 – 22 §§ (se avsnitt 8.8).
- Incidenthantering 3 kap. 17 § (se avsnitt 7.7).

8.9 Skydd mot skadlig kod 4 kap. 24 §

8.9.1 Introduktion

Skydd mot skadlig kod är en central del av cybersäkerhetsarbetet och syftar till att förebygga, upptäcka och begränsa påverkan från exempelvis virus, ransomware och annan skadlig programvara. Genom att införa tekniska skyddsåtgärder och löpande övervaka hot kan organisationen minska risken för att system och information komprometteras.

Brister i skyddet mot skadlig kod kan leda till informationsläckor, obehörig åtkomst, driftstörningar och omfattande verksamhetspåverkan, särskilt om skadlig kod får möjlighet att spridas mellan system och nätverkssegment.

8.9.2 Krav

4 kap. 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.

8.9.3 Tolkningsstöd

Begrepp och formuleringar

För tolkningsstöd rörande begreppen system samt it- och ot-segment, se begreppslistan.

Tillgänglig på marknaden

Stöd för bedömningen om en mjukvara är tillgänglig på marknaden är exempelvis om den är färdigutvecklad för distribution, kan användas med stöd av standardiserade licensavtal och är fritt tillgänglig för målgruppen att anskaffa, exempelvis hos en återförsäljare.

8.9.4 Kopplingar till andra paragrafer

Närmare om:

- Säkerhetskonfigurering 4 kap. 13 § (se avsnitt 8.5).

8.10 Kryptering 4 kap. 25–26 §§

8.10.1 Introduktion

Kryptering är en viktig säkerhetsåtgärd för att skydda information mot obehörig åtkomst när den lagras, behandlas eller överförs mellan system. Kryptering utgör även en central komponent i många autentiseringslösningar genom att möjliggöra säker verifiering av användare, system och tjänster samt skydda autentiseringsuppgifter från att avlyssnas eller manipuleras. Den snabba tekniska utvecklingen, med ökande mängder data, fler digitala tjänster och mer avancerade cyberhot, ställer samtidigt krav på att kryptografiska lösningar löpande utvärderas, uppdateras och anpassas till nya hot.

Brister i användningen eller hanteringen av kryptering kan leda till informationsläckor, obehörig åtkomst, försvagad autentisering, bristande regelefterlevnad och ökad påverkan vid säkerhetsincidenter.

8.10.2 Krav

4 kap. 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.

4 kap. 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.

8.10.3 Tolkningsstöd

Begrepp och formuleringar

För tolkningsstöd rörande begreppen identifiera och hantera samt digital miljö se begreppslistan.

Kvantkryptering

Den tekniska utvecklingen på krypteringsområdet går fort och möjligheter och utmaningar kring kvanttekniken inom kryptering analyseras löpande, bland annat av FRA. Det rekommenderas att verksamhetsutövarna följer de råd som NCSC/FRA utfärdar på området.

Uppenbart obehövligt att använda DNSSEC

Kravet innebär att verksamhetsutövaren ska använda DNSSEC för att hindra manipulering av DNS. Verksamhetsutövaren behöver bedöma vilka system

som ska vara externt tillgängliga och därmed tilldelas ip-adress i DNS-systemet.

Interna informationssystem är nåbara via verksamhetsutövarensinterna nät. För att hålla ordning på system och ip-adresser i det interna nätverket behövs ofta motsvarande funktionalitet som DNS ger på internet. Verksamhetsutövaren behöver se till att de interna systemen inte är nåbara externt och inte registrerade i DNS. Om sådan registrering görs, vilket också innebär att systemen går att slå upp och därmed blir synliga externt, krävs DNSSEC.

Det är inte helt givet i vilka fall det skulle kunna vara uppenbart obehövligt att använda DNSSEC för sådana system som ska vara externt åtkomliga. Om en verksamhetsutövare har registrerat ett domännamn i domännamnssystemet och vid en riskbedömning inte identifierar någon problematik för vare sig själv eller någon annan om domännamnet förfalskas och trafikleds fel kan det eventuellt vara ett sådant fall. Det är tillsynsmyndigheten som avgör i det enskilda fallet.

8.10.4 Kopplingar till andra paragrafer

Närmare om:

- omvärldsbevakning och kravet att följa information från NCSC/FRA, 3 kap. 10 § (se avsnitt 7.3).
- Segmentering och skydd av externt tillgängliga system 4 kap 11 § (se avsnitt 8.4).
- innebörd och hantering av autentiseringsuppgifter 4 kap. 14, 16 – 17 §§ (se avsnitt 8.6).

8.11 Säkerhetstester och granskningar 4 kap. 27 §

8.11.1 Introduktion

Säkerhetstester och säkerhetsgranskningar är viktiga för att identifiera sårbarheter, felaktiga konfigurationer och andra brister innan de kan utnyttjas av angripare eller orsaka störningar i verksamheten. Genom regelbundna tester och granskningar kan organisationen verifiera att säkerhetsåtgärder fungerar som avsett och att risker hanteras på ett effektivt sätt.

Brister i säkerhetstester och granskningar kan leda till att sårbarheter förblir oupptäckta, vilket ökar risken för cyberangrepp, informationsläckor, driftstörningar och felaktiga riskbedömningar.

8.11.2 Krav

4 kap 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 driftrelaterade 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.

8.11.3 Tolkningsstöd

Begrepp och formuleringar

För tolkningsstöd rörande begreppen cybersäkerhet, lämpliga och proportionerliga säkerhetsåtgärder, system, it- och ot-segment, samt digital miljö se begreppslistan.

Säkerhetstester och granskningar

Säkerhetstester och granskningar kan göras på olika sätt, med olika syften och omfattning. Huvudsyftet är att upptäcka brister avseende skyddet för konfidentialitet, riktighet och tillgänglighet. Säkerhetstester och granskningar kompletterar varandra.

Säkerhetstester, såsom begreppet används i föreskrifterna, syftar till att finna tekniska sårbarheter och genomförs i huvudsak genom sårbarhetsskanningar och intrångstester (penetrationstester eller pentest).

Granskningar, såsom begreppet används i föreskrifterna, innebär en manuell granskning av dokumentation i syfte att hitta fel och brister. Det kan exempelvis handla om att granska kod, konfigurationer, arkitektur och brandväggsregler. Det innefattar också kontroll av att den dokumentation som

beskriver den digitala miljön och informationssystemen är tillräcklig för att drift och förvaltning ska kunna bedrivas på ett säkert sätt.

Publicerade sårbarheter

Med publicerade sårbarheter åsyftas i föreskrifterna sådana sårbarheter som tillgängliggjorts i etablerade kanaler för sådan typ av informationsspridning tillsammans med nödvändig säkerhetsuppdatering. Det vill säga det handlar inte om så kallade zero-day-sårbarhet, sårbarheter där leverantören ännu inte publicerat en lösning.

Systemens behov av cybersäkerhet

Ledning för vilket behov av cybersäkerhet ett visst system har kan hämtas från bland annat ledningens inriktning, de behov som informationsägaren formulerat och riskbedömningar.

Rapportera sårbarheter

Vid säkerhetstester och granskningar kan sårbarheter upptäckas som inte tidigare publicerats. I dessa fall är det av vikt att dela information om sårbarheterna för att lösningar skyndsamt ska kunna tas fram. CSIRT-enheten hos nationellt cybersäkerhetscenter (NCSC) har i uppdrag att ta emot rapporter om sårbarheter. Vem som rapporterar in en sårbarhet omfattas av sekretessbestämmelser hos NCSC.

8.11.4 Kopplingar till andra paragrafer

Närmare om:

- omvärldsbevakning och kravet att följa information från NCSC/FRA, 3 kap. 10 § (se avsnitt 7.3).
- Segmentering och skydd av externt tillgängliga system 4 kap. 11 § (se avsnitt 8.4).

8.12 Återställning av förlorad information och säkerhetskopiering 4 kap. 28 §

8.12.1 Introduktion

Återställning av förlorad information och säkerhetskopiering är avgörande för att säkerställa verksamhetens motståndskraft vid cyberangrepp, systemfel, mänskliga misstag eller andra störningar. Genom att regelbundet säkerhetskopiera information och verifiera att återställning fungerar kan organisationen återuppta verksamheten och begränsa konsekvenserna av incidenter. Brister i säkerhetskopiering eller återställningsförmåga kan leda till permanent informationsförlust, förlängda driftavbrott, verksamhetsstörningar,

ekonomiska förluster och ökad påverkan vid exempelvis ransomwareangrepp eller andra säkerhetsincidenter.

8.12.2 Krav

4 kap. 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.

8.12.3 Tolkningsstöd

Begrepp och formuleringar

För tolkningsstöd rörande begreppet system, identifiera och hantera behovet, acceptabla tider för otillgänglighet och bristande funktionalitet, se begreppslistan.

Återställning av information utan värde

Hur återställning ska göras ska utgå från informationens värde för verksamhetsutövaren. Om verksamhetsutövaren exempelvis blivit av med information som enligt de fastställda acceptabla tiderna för otillgänglighet och bristande funktionalitet inte behöver återställas är det inte nödvändigt att göra en sådan.

Krav på säkerhetskopiering

Föreskrifterna innebär inte några krav på att återställning måste göras med stöd av säkerhetskopiering. Återställning kan även göras på andra sätt. Om det exempelvis är information som verksamhetsutövaren enklast återställer genom att hämta in den från en extern aktör så behöver inte verksamhetsutövaren ha egna säkerhetskopior.

8.12.4 Kopplingar till andra paragrafer

Närmare om:

- Acceptabla tider för otillgänglighet och bristande funktionalitet 3 kap. 7 och 15 §§ (se avsnitt 7.3).

8.13 Intrångsdetektering och intrångsskydd 4 kap. 29 §

8.13.1 Introduktion

Intrångsdetektering och intrångsskydd är viktiga säkerhetsåtgärder för att upptäcka, förhindra och begränsa effekterna av obehöriga aktiviteter och cyberangrepp mot verksamhetens system och nätverk. Genom att övervaka trafik, identifiera avvikelser och blockera misstänkta aktiviteter kan organisationen förbättra sin förmåga att upptäcka och hantera säkerhetsincidenter innan de får allvarliga konsekvenser.

Brister i intrångsdetektering och intrångsskydd kan leda till att angrepp förblir oupptäckta eller inte stoppas i tid, vilket ökar risken för informationsläckor, obehörig åtkomst, driftstörningar och omfattande verksamhetspåverkan.

8.13.2 Krav

4 kap. 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 intrångs detektering och intrångsskydd för ot-segment i produktionsmiljön.

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

8.13.3 Tolkningsstöd

Begrepp och formuleringar

För tolkningsstöd rörande begreppen it-segment, ot-segment, produktionsmiljö, utvecklings-, test- och utbildningsmiljö samt identifiera och hantera, se begreppslistan.

Intrångsdetektering och intrångsskydd

Intrångsdetektering syftar till att upptäcka försök till och genomförda intrång. Intrångsdetekteringssystemet kan kompletteras med intrångsskydd som ger möjlighet att även agera på upptäckta försök till intrång, exempelvis genom att direkt blockera angreppet. Intrång som kan antas ha en brottslig grund ska polisanmälas.

Arbetet underlättas av bland annat av ändamålsenlig segmentering och säkerhetskonfigurering samt incident- och krishantering.

Föreskriften ställer inga krav på att verksamhetsutövarna ska ha en specifik teknisk lösning, utan endast på att verksamhetsutövaren ska använda intrångsdetektering och intrångsskydd.

8.13.4 Kopplingar till andra paragrafer

Närmare om:

- Incident- och krishantering 3 kap. 17 – 18 §§ (se avsnitt 7.7 och 7.8).
- Segmentering 4 kap. 11 – 12 §§ (se avsnitt 8.4).
- Säkerhetskonfigurering 4 kap. 13 § (se avsnitt 8.5).

8.14 Ändringshantering 4 kap. 30 – 31 §§

8.14.1 Introduktion

Ändringshantering är en viktig del av cybersäkerhetsarbetet och syftar till att säkerställa att förändringar i system, nätverk och konfigurationer genomförs på ett kontrollerat och säkert sätt. Genom tydliga processer för planering, riskbedömning, testning och godkännande av förändringar minskas risken för att nya sårbarheter, fel eller driftstörningar introduceras i den digitala miljön.

Brister i ändringshanteringen kan leda till oavsiktliga säkerhetsbrister, försvagad säkerhetsnivå, systemfel och verksamhetsstörningar samt försvåra spårbarhet och incidenthantering.

8.14.2 Krav

4 kap. 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.

4 kap. 31 §

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

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

Allmänna råd

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

8.14.3 Tolkningsstöd

Begrepp och formuleringar

För tolkningsstöd rörande begreppen skyndsamt, produktionsmiljö, utvecklings-, test- och utbildningsmiljö, identifiera och hantera samt utan onödigt dröjsmål, se begreppslistan.

Uppgradering och uppdatering

Med uppdatering avses en installation av leverantörens senaste version av en mjukvara som redan finns i informationssystemet. Med uppgradering avses att gammal hård- eller mjukvara byts ut och ersätts med en ny lösning.

Säkerhetsuppdateringar är en särskild typ av uppdateringar. Säkerhetsuppdateringar innehåller uppdateringar som stärker cybersäkerheten, exempelvis genom att åtgärda en sårbarhet eller introducera en ny säkerhetsfunktionalitet.

8.14.4Kopplingar till andra paragrafer

Närmare om:

- Systemägarens ansvar för system under hela dess livslängd 3 kap. 8 § (se avsnitt 7.3).
- Säkerhet vid utveckling och drift 4 kap. 5 § (se avsnitt 8.2).

9 Femte kapitlet Fysiska säkerhetsåtgärder

9.1 Lokaler 5 kap. 1–3 §§

9.1.1 Introduktion

Skydd av organisationens lokaler är en viktig del av cybersäkerhetsarbetet eftersom informationssystem, nätverksutrustning, lagringsmedier och annan kritisk infrastruktur är beroende av både fysisk säkerhet och en stabil driftmiljö. Skyddet omfattar inte bara att förhindra obehörig åtkomst, stöld och sabotage, utan även att motverka skador från exempelvis brand, översvämning, vattenläckage, strömavbrott och andra miljörelaterade händelser.

Brister i det fysiska skyddet kan leda till informationsläckor, förlust av utrustning, driftstörningar, avbrott i samhällsviktiga tjänster och omfattande verksamhetspåverkan till följd av både avsiktliga handlingar och oavsiktliga händelser.

9.1.2 Krav

5 kap. 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.

5 kap. 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.

5 kap. 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.

9.1.3 Tolkningsstöd

Begrepp och formuleringar

För tolkningsstöd rörande begreppen säkerställa, identifiera och hantera, särskilda it- och ot-utrymmen, om inte uppenbart obehövligt samt information i behov av utökat skydd se begreppslistan.

Bevakning

Föreskrifterna ställer krav på att vissa utrymmen ska förses med bevakning. Med bevakning i dessa fall avses fysisk övervakning, i form av exempelvis en vakt eller liknande.

Verksamhetens lokaler

Kravet i föreskrifterna att skydda lokaler mot obehörigt tillträde gäller oavsett om verksamhetsutövaren äger lokalerna eller endast hyr dessa. I det senare fallet uppfylls kravet lämpligen genom att ställa adekvata krav på uthyraren. Är detta inte möjligt kan kompensatoriska åtgärder vidtas, exempelvis förstärkt larm. Hur skyddet behöver utformas bestäms lämpligen utifrån externa krav, interna behov och identifierade risker.

Med tillträdesbegränsning avses exempelvis grindar, lås och staket.

Utpekade besöksutrymmen

Verksamhetsutövaren pekar ut besöksutrymmen utifrån sina egna behov och verksamheter. Omfattningen kan skilja sig åt mellan olika verksamheter. Många offentliga verksamhetsutövare har ett större behov av att vara tillgängliga för allmänheten än verksamhetsutövare i privat sektor. Styrande vid beslut om vad som ska pekas ut som besöksutrymmen är risken för obehörig fysisk åtkomst till, förlust av och fysisk skada på system.

Föreskrifterna utgör inte något hinder att ge besökare tillgång till andra delar av verksamhetsutövarens lokaler men då krävs att identiteten kontrolleras. Sådan kontroll kan exempelvis göras genom uppvisande av identitetshandling.

Sektioner skilda från verksamhetsutövarens övriga lokaler

Kravet i det allmänna rådet syftar till att skydda information i behov av utökat skydd från att bli tillgänglig för obehöriga, exempelvis genom att ligga lättillgänglig vid skrivare eller att obehöriga kan ställa sig bakom ryggen på medarbetare som arbetar med informationen och läsa den. Sektionering kan uppnås på flera olika sätt, det handlar inte bara om olika rum utan kan även utgöras av insynsskydd av olika slag. Ledning för utformningen hämtas lämpligen i informationsklassning och riskanalys.

Fysiska säkerhetsåtgärder där verksamhetsutövaren saknar rådighet över lokalerna

Läs mer om utkontraktering av informationsbehandling i avsnitt 8.1.

9.1.4 Kopplingar till andra paragrafer

Närmare om:

- Informationsklassning, 3 kap. 11 § (se avsnitt 7.4).
- Riskhantering, 3 kap. 12–13 §§ (se avsnitt 7.5).

9.2 Tekniska försörjningssystem 5 kap. 4 §

9.2.1 Introduktion

Tillräcklig funktionalitet avseende elförsörjning, kyla, värme, ventilation samt externa elektroniska kommunikationsnät och kommunikationstjänster är en grundläggande förutsättning för säker och stabil drift av organisationens digitala miljö. Dessa stödtjänster möjliggör att informationssystem, nätverksutrustning och digitala tjänster kan fungera som avsett även under störda förhållanden.

Brister i funktionaliteten eller störningar i dessa beroenden kan leda till avbrott i verksamhetskritiska system, förlorad tillgänglighet till information och tjänster, försämrad förmåga att upptäcka och hantera säkerhetsincidenter samt betydande verksamhetsstörningar med ekonomiska och operativa konsekvenser.

9.2.2 Krav

5 kap. 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.

9.2.3 Tolkningsstöd

Begrepp och formuleringar

För tolkningsstöd rörande begreppen system, digital miljö, identifiera och hantera, se begreppslista.

Tekniska försörjningssystem

Tekniska försörjningsystem är de system som är avgörande, direkt eller indirekt, för upprätthållandet av en viktig samhällsfunktion. Det kan vara system som styr eller bidrar till funktionen för exempelvis dricksvatten, avlopp, elektricitet, datanät eller fjärrvärme och fjärrkyla.

Tillräcklig funktionalitet

Om ett sektorskritiskt system är beroende av ett tekniskt försörjningssystem för att upprätthålla tillräcklig funktionalitet, ska verksamhetsutövaren betrakta det tekniska försörjningssystemet och de digitala system som behövs för dess funktion som sektorskritiska i den utsträckning beroendet kräver.

Redundanta funktioner

En funktion som mer eller mindre automatiskt kan ersätta den ursprungliga funktionen i ett system. Det kan exempelvis vara inbyggda komponenter i ett system som gör att ett system vid exempelvis överhettning byter server till en annan som kyls i ett separat system.

9.2.4 Kopplingar till andra paragrafer

10 Sjätte kapitlet Sektorsspecifika säkerhetsåtgärder

10.1 Offentlig förvaltning

Kapitel 10 är endast tillämpligt på verksamhetsutövare inom sektors offentlig förvaltning.

10.2 System för kriskommunikation 6 kap. 1–2 §§

10.2.1 Introduktion

System för kriskommunikation är en viktig förutsättning för att offentliga verksamheter ska kunna leda, samordna och upprätthålla verksamheten vid allvarliga störningar, kriser eller höjd beredskap. Genom robusta och tillgängliga kommunikationslösningar kan information snabbt förmedlas mellan berörda aktörer, medarbetare, beslutsfattare och allmänheten även när ordinarie kommunikationskanaler är begränsade eller otillgängliga.

Brister i funktionaliteten hos system för kriskommunikation kan leda till fördröjd eller felaktig informationsdelning, bristande samordning, försvårat beslutsfattande och minskad förmåga att hantera incidenter och kriser, vilket kan få betydande konsekvenser för verksamheten och samhället.

10.2.2 Krav

6 kap. 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.

6 kap. 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.

10.2.3 Tolkningsstöd

Begrepp och formuleringar

För tolkningsstöd rörande begreppen cybersäkerhet, system, identifiera och hantera, se begreppslista.

Offentlig förvaltnings ansvar att kommunicera

Offentlig förvaltning har ett ansvar att kunna kommunicera med allmänheten även under en pågående kris.

Kriskommunikation

Kriskommunikation är sådan information som ger medborgarna den information som de behöver för att kunna känna sig informerade om krisen, och vilka, om några, åtgärder som behöver vidtas för att minimera de krisens negativa effekter. Kriskommunikation kan användas både internt, inom verksamhetsutövarens verksamhet, eller externt, till allmänheten. Vad kriskommunikationen inkluderar och omfattar kan däremot skilja sig beroende på om det rör sig om intern eller extern kriskommunikation. Vilken information som är lämplig att dela med vilken krets och i vilket skede är upp till respektive verksamhetsutövare.

Rakelterminaler och SWEN-terminaler

Rakel är Sveriges nationella kommunikationssystem för samverkan och ledning. Med Rakel kan medarbetare med samhällsviktiga uppdrag kommunicera säkert och effektivt i vardag och kris. Rakel är byggt för att klara tuffa väderförhållanden och är anpassat för verksamheter med särskilt höga krav på säkerhet och robusthet. Rakelsystemet har extremt hög tillgänglighet. Vid längre strömavbrott exempelvis, fortsätter systemet att drivas med hjälp av en väl planerad reservkraft.

Myndigheten för civilt försvar etablerar SWEN som ska bli nästa generations nationella kommunikationsnätverk för samhällsviktiga aktörer. SWEN ska stegvis ersätta dagens Rakel och övergången förväntas vara klar till 2030.

SGSI är en avgiftsfinansierad kommunikationstjänst, skild från internet, för säker och krypterad kommunikation mellan användare i Sverige och Europa.

10.2.4 Kopplingar till andra paragrafer

Närmare om:

- Personalsäkerhet, 3 kap. 9 § (se avsnitt 7.3).

11 Sjunde kapitlet Undantag

11.1.1 Krav

7 kap. 1 §

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

11.1.2 Tolkningsstöd

Försvarets radioanstalt avgör när särskilda fall föreligger.