Notera att denna skrivelse utgör ett tillägg till den efterfrågade Excelfilen. Syftet med tillägget är att fördjupa och utveckla resonemanget samt därigenom ytterligare stödja MCF:s arbete.

Remissyttrande - Förslag till föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning enligt cybersäkerhetslag (2025:1506)

Diarienummer: MCF 2026-04554

1. Sammanfattning

Säkerhets- och försvarsföretagen (SOFF) och Teknikföretagen välkomnar att Myndigheten för civilt försvar tar fram föreskrifter och allmänna råd som konkretiserar cybersäkerhetslagens krav på säkerhetsåtgärder och ledningens utbildning. Ett tydligt, riskbaserat och harmoniserat regelverk är viktigt för Sveriges cybersäkerhet, totalförsvarsförmåga, samhällsviktiga verksamheter och företagens konkurrenskraft.

Vi är positiva till att förslaget i flera delar utgår från ett systematiskt och riskbaserat arbetssätt, att det tydliggör ledningens ansvar och att det knyter an till etablerade standarder. Förslaget innehåller också flera relevanta kravområden, bland annat incidenthantering, kontinuitet, leveranskedjesäkerhet, åtkomstkontroll, loggning, säker utveckling och skydd av OT-miljöer.

Samtidigt bedömer vi att förslaget behöver justeras i vissa delar för att bli mer rättssäkert, proportionerligt, teknikneutralt och praktiskt genomförbart. Det gäller särskilt krav som riskerar att bli detaljstyrande, snabbt tekniskt föråldrade eller svåra att tillämpa i internationella koncerner, försvarsindustriella leveranskedjor, OT-miljöer, molnmiljöer och SME-företag.

EU:s inre marknad är svenska företags hemmamarknad, och omkring tre fjärdedelar av Sveriges utrikeshandel sker med övriga EU-länder. Den fria rörligheten, gemensamma produktregler och lika konkurrensvillkor har skapat en marknadsintegration och handel som är avgörande för en internationellt konkurrenskraftig industri i Sverige. Grundläggande för detta är fri rörlighet och harmoniserad lagstiftning – det vill säga att regelverk både utformas och tillämpas likartat i alla medlemsstater. Mot denna bakgrund är överimplementering och nationella särkrav problematiska. Även om EU-direktiv kan medge utrymme för nationella kompletteringar anser Teknikföretagen och SOFF att genomförandet i Sverige bör ske i linje med vad som överenskommits på EU-nivå. Det är angeläget att avhålla sig från att införa ytterligare krav, inte minst för att undvika att svenska företag ges sämre konkurrensvillkor än sina europeiska konkurrenter. Genomförandet måste därför utformas så att svenska företags konkurrenskraft inom EU:s inre marknad inte försämras. Det måste också säkerställas att

tillämpning och tillsyn inom Sveriges gränser, mellan olika ansvariga tillsynsmyndigheter, sker på ett likartat sätt för att undvika snedvridningar och konkurrensproblematik inom landet.

SOFF och Teknikföretagen föreslår sammanfattningsvis att MCF:

1. Förtydligar relationen till annan reglering, särskilt säkerhetsskyddslagstiftningen, DORA, sektorsreglering, exportkontroll, upphandlingskrav och internationella krav.
2. Säkerställer att kraven kan uppfyllas genom användande av etablerade standarder, ramverk och certifieringar, exempelvis ISO/IEC 27001, ISO/IEC 27002, NIST CSF och motsvarande.
3. Överväger att omvandla (delar av) föreskrifterna till allmänna råd, för att skapa en större flexibilitet vid genomförande av åtgärder. Om det inte är möjligt är det viktigt att MCF tydligare skiljer mellan bindande *föreskriftskrav* och *vägledande exempel*.
4. Minskar risken för dubbelreglering genom att erkänna likvärdiga eller mer långtgående krav enligt annan reglering eller kontraktuella säkerhetskrav.
5. Förtydligar att krav ska kunna uppfyllas genom riskbaserade, funktionsbaserade och teknikneutrala kontroller, inte enbart genom de tekniska lösningar som nämns i förslaget.
6. Anpassar kraven för verksamheter med OT, äldre system, säkerhetsskyddsklassificerade uppgifter, försvarsmateriel, internationella leveranskedjor och globala IT-miljöer.
7. Kompletterar konsekvensutredningen med en fördjupad analys av kostnader och genomförbarhet för SME-företag, försvars- och säkerhetsföretag, internationellt verksamma företag och leverantörskedjor.
8. Inför tydliga övergångsbestämmelser och ett stegvis införande, särskilt för avtal, äldre system, OT-miljöer och leverantörskrav.
9. Tar initiativ till att ansvariga tillsynsmyndigheter upprätthåller och skapar forum för att säkerställa likartad tolkning och tillämpning av föreskrifter och råd framgent.

SOFF och Teknikföretagen tillstyrker således inriktningen i förslaget, men avstyrker att föreskrifterna beslutas i nuvarande formulering utan de förtydliganden och ändringar som anges nedan.

2. Övergripande synpunkter

2.1 Ett tydligt regelverk är nödvändigt men måste vara proportionerligt

Cybersäkerhetslagen kräver att verksamhetsutövare vidtar lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska säkerhetsåtgärder. Kraven ska utgå från ett

allriskperspektiv och säkerställa en nivå som är lämplig i förhållande till risken. Lagen anger också att åtgärderna åtminstone ska avse bland annat riskanalys, incidenthantering, kontinuitet, leveranskedjesäkerhet, säker utveckling, cyberhygien, kryptografi, åtkomstkontroll och autentisering.

Det är därför viktigt att föreskrifterna inte omvandlar ett riskbaserat krav till ett generellt kontrollbibliotek där samtliga verksamhetsutövare förväntas införa samma tekniska och administrativa lösningar oberoende av verksamhet, storlek, systemmiljö, hotbild och faktisk risk. För företag är förmågan att prioritera åtgärder efter risk avgörande för att säkerhetsarbetet ska bli effektivt och inte tränga undan investeringar i andra skyddsåtgärder med högre riskreducerande effekt. Av denna anledning ser vi att delar av föreskrifterna skulle kunna ändras till allmänna råd, för att möjliggöra en större flexibilitet vid genomförandet.

2.2 Förslaget har flera positiva delar

SOFF och Teknikföretagen ser positivt på att förslaget:

- utgår från ett systematiskt och riskbaserat cybersäkerhetsarbete,
- anger att arbetet ska integreras med befintligt sätt att leda och styra organisationen,
- tydliggör ledningens roll i att fastställa mål, inriktning och uppföljning,
- erkänner betydelsen av etablerade standarder,
- omfattar både organisatoriska, tekniska, driftsrelaterade och fysiska åtgärder,
- lyfter leveranskedjor, utkontraktering och incidenthantering,
- särskilt uppmärksammar IT- och OT-miljöer,
- i flera delar använder formuleringen “identifiera och hantera behovet av”, vilket stödjer ett riskbaserat arbetssätt.

MCF:s förslag innehåller uttryckliga krav på systematiskt och riskbaserat arbete, integrering med befintlig styrning samt identifiering och hantering av behovet av relevanta standarder. I allmänna råd nämns ISO/IEC 27001 och ISO/IEC 27002 som stöd.

2.3 Vissa krav riskerar att bli mer långtgående än NIS2:s riskbaserade modell

NIS2 och cybersäkerhetslagen bygger på lämpliga och proportionella åtgärder. MCF:s föreskrifter bör därför i högre grad renodla kravens funktion och önskade effekt, medan detaljerade exempel på tekniska lösningar bör placeras i allmänna råd eller vägledning.

Exempel på krav som bör ses över är:

- obligatorisk anslutning till specifika nationella tjänster,
- krav som utgår från specifika tekniker eller tekniska arkitekturer,

- mycket detaljerade dokumentationskrav,
- krav på certifiering där relevanta certifieringsordningar ännu saknas,
- krav på åtgärdstider som inte tar hänsyn till OT, säkerhetskritiska system eller leverantörsberoenden,
- krav som riskerar att förutsätta en offentligförvaltningsmodell för styrning även hos privata företag.

3. Relation till annan reglering och risk för dubbelreglering

3.1 Krav enligt annan författning bör erkännas om de har motsvarande verkan

Förslagets 1 kap. 2 § anger att om annan författning innehåller bestämmelser som ställer högre krav än dessa föreskrifter ska den bestämmelsen tillämpas. Detta är otillräckligt. Cybersäkerhetslagen anger att om annan författning innehåller krav på säkerhetsåtgärder eller incidentrapportering ska dessa bestämmelser gälla om verkan av kraven minst motsvarar verkan av skyldigheterna enligt cybersäkerhetslagen, med beaktande av omfattning, tillsyn och sanktioner.

Föreskrifterna bör därför inte endast hänvisa till “högre krav”, utan även till likvärdiga krav med motsvarande verkan. Annars riskerar verksamhetsutövare att behöva visa efterlevnad enligt flera parallella regelverk trots att samma risk redan hanteras genom annan reglering.

Detta är särskilt viktigt för företag som omfattas av eller påverkas av:

- säkerhetsskyddslagstiftningen,
- DORA och finansiell reglering,
- exportkontroll och försvarskundkrav,
- luftfarts-, rymd-, energi-, transport- och telekomreglering,
- upphandlingsrättsliga säkerhetskrav,
- internationella kund- och myndighetskrav,
- Nato-, EU- och krav inom försvars- och säkerhetsområdet.

Föreslagen alternativ formulering av 1 kap. 2 §:

Om annan författning innehåller bestämmelser om säkerhetsåtgärder, incidenthantering, kontinuitet, informationssäkerhet eller motsvarande som till sin verkan minst motsvarar kraven i dessa föreskrifter, får verksamhetsutövaren beakta sådan efterlevnad vid bedömningen av om kraven enligt dessa föreskrifter är uppfyllda. Om annan författning ställer mer långtgående krav ska dessa krav tillämpas i den delen.

3.2 Relation till säkerhetsskyddslagstiftningen måste förtydligas

Försvars- och säkerhetsföretag bedriver ofta verksamhet där delar omfattas av säkerhetsskyddslagen, medan andra delar omfattas av cybersäkerhetslagen. Cybersäkerhetslagen innehåller undantag för verksamheter som enbart bedriver säkerhetskänslig verksamhet och anger också att skyldigheterna enligt 2 kap. 3–10 §§ inte gäller för den delen av verksamheten som är säkerhetskänslig. Uppgifter som är säkerhetsskyddsklassificerade undantas också från skyldigheten att lämna uppgifter enligt cybersäkerhetslagen.

I praktiken är gränsdragningen ofta komplex. Ett företag kan ha gemensam IT-infrastruktur, gemensamma SOC-funktioner, gemensamma leverantörer och gemensamma ledningssystem för både säkerhetskänslig och icke säkerhetskänslig verksamhet. MCF bör därför ta fram vägledning om hur verksamhetsutövare ska:

- avgränsa den del av verksamheten som omfattas av cybersäkerhetslagen,
- hantera gemensamma stödsystem som används av både säkerhetskänslig och annan verksamhet,
- visa efterlevnad utan att röja säkerhetsskyddsklassificerade uppgifter,
- undvika motstridiga krav mellan tillsyn enligt cybersäkerhetslagen och tillsyn enligt säkerhetsskyddslagstiftningen,
- hantera incidenter som berör både cybersäkerhetslagen och säkerhetsskyddslagen,
- tillämpa säkerhetsskyddsavtal och leverantörskrav i relation till föreskrifternas krav på leveranskedjor.

Rekommendation: MCF bör, i samråd med Säkerhetspolisen, Försvarsmakten, tillsynsmyndigheter och näringslivet, ta fram särskild vägledning för företag som bedriver både säkerhetskänslig och icke säkerhetskänslig verksamhet.

4. Proportionalitet, teknikneutralitet och praktisk tillämpbarhet

4.1 Kraven bör uttryckas funktionsbaserat

Flera krav är lämpligt formulerade genom att ange vilken effekt som ska uppnås. Andra krav pekar däremot ut specifika tekniska lösningar eller processer. Sådana krav bör endast vara bindande när tekniken är stabil, allmänt tillgänglig och nödvändig för att uppnå lagens syfte.

Exempel där teknikneutraliteten bör stärkas:

- robust och korrekt tid bör kunna uppfyllas genom tid som är spårbar till UTC, inte enbart genom svensk UTC-tillämpning eller viss tidstjänst,
- segmentering bör kunna ske genom fysisk, logisk, identitetsbaserad eller annan teknisk separation,

- intrångsdetektering bör kunna uppfyllas genom IDS, EDR, XDR, SIEM, nätverksövervakning, OT-anpassad passiv monitorering eller motsvarande,
- skydd mot skadlig kod bör omfatta moderna endpoint-, applikationskontroll- och övervakningslösningar, inte enbart traditionell antivirusmjukvara,
- säkerhetskopiering bör kunna uppfyllas genom offline-, immutable-, air-gapped- eller motsvarande skydd.

4.2 MCF bör tydligare erkänna etablerade standarder och ramverk

Förslaget nämner ISO/IEC 27001 och ISO/IEC 27002. Detta är positivt men otillräckligt, särskilt för industriföretag, försvarsföretag och OT-verksamhet. MCF bör uttryckligen ange att även andra etablerade standarder och ramverk kan användas när de är relevanta.

Föreslagen komplettering till 3 kap. 2 § eller allmänt råd:

Som stöd för arbetet kan verksamhetsutövaren använda relevanta europeiska och internationella standarder, ramverk och branschpraxis, exempelvis SS-ISO/IEC 27001, SS-EN ISO/IEC 27002, ISO/IEC 27005, ISO 22301, IEC 62443, NIST Cybersecurity Framework, NIST SP 800-serien, CIS Controls eller motsvarande. Val av standarder bör utgå från verksamhetens art, storlek, systemmiljö, hotbild och risker.

MCF bör också klargöra att certifiering enligt en standard inte automatiskt innebär full efterlevnad, men att certifiering, tredjepartsgranskning eller etablerad kontrollmappning bör kunna användas som bevisning vid tillsyn.

5. Särskilda konsekvenser för olika företagstyper

5.1 Stora företag och koncerner

Stora företag har ofta globala ledningssystem, gemensamma IT-plattformar, koncernövergripande SOC, centraliserad identitetsstyrning, internationella molntjänster och matrisorganisationer. Föreskrifterna bör därför uttryckligen medge att krav kan uppfyllas genom koncerngemensamma processer, gemensamma funktioner och globala kontroller, förutsatt att den svenska verksamhetsutövaren kan visa att kraven uppfylls för den verksamhet som omfattas.

Utan ett sådant förtydligande riskerar kraven att leda till dubbel dokumentation, dubbla roller och parallella processer för svenska enheter, trots att säkerheten i praktiken hanteras mer effektivt på koncernnivå.

5.2 SME-företag

SME-företag träffas både direkt och indirekt. Även om vissa mindre företag inte omfattas direkt av cybersäkerhetslagen kan de påverkas genom krav från större kunder, myndigheter, huvudleverantörer och samhällsviktiga verksamheter. Leverantörskrav kan därmed få betydande kaskadeffekter.

MCF:s konsekvensutredning konstaterar att det är svårt att göra generellt giltiga uppskattningar av resursbehovet för cybersäkerhet och att kostnader kan avse utrustning, programvara, personal, revisioner och utbildningar. För SME-företag kan även mindre administrativa krav få stora konsekvenser, särskilt om flera kunder ställer olika versioner av samma krav.

MCF bör därför:

- ta fram förenklade vägledningar för SME-företag,
- tillhandahålla exempel på riskbaserad miniminivå,
- utveckla mallar för leverantörskrav,
- undvika krav som förutsätter stora GRC-organisationer,
- tydliggöra att kontrollnivå och dokumentationsnivå ska stå i proportion till risk.

5.3 Försvars- och säkerhetsföretag

Försvars- och säkerhetsföretag verkar i ett särskilt komplext regelverk. Företagen hanterar ofta säkerhetskänslig verksamhet, exportkontrollerad information, försvarsmateriel, internationella säkerhetskrav, upphandlingskrav, säkerhetsskyddsavtal och kundspecifika cyberkrav från svenska och utländska myndigheter.

Föreskrifterna bör därför inte utformas så att de skapar parallella, delvis motstridiga krav ovanpå redan långtgående krav enligt säkerhetsskydd, försvarsupphandling, exportkontroll och internationella kundkrav. I stället bör MCF ange hur sådana krav kan beaktas som del av efterlevnaden.

Särskilt viktigt är att krav på incidentrapportering, sårbarhetsrapportering, leverantörsinformation och tillsynsunderlag inte leder till att säkerhetsskyddsklassificerade uppgifter, affärskritisk information, exportkontrollerad information eller försvarssekretess röjs.

5.4 Internationellt verksamma företag

Internationella företag kan omfattas av flera nationella NIS2-implementeringar och andra cybersäkerhetsregelverk. Sverige bör undvika särkrav som avviker från NIS2:s riskbaserade och teknikneutrala modell, eftersom sådana avvikelser kan skapa fragmentering, ökade kostnader och minskad konkurrenskraft.

Det bör tydliggöras att internationella koncerngemensamma kontroller, standardiserade policyer, globala incidentprocesser, internationellt erkända certifieringar och centraliserade säkerhetsfunktioner kan användas för att uppfylla svenska krav.

5.5 Leverantörskedjor

Förslaget innehåller långtgående krav på leverantörer och utkontraktering. MCF föreslår bland annat att verksamhetsutövaren ska utvärdera potentiella leverantörer innan förvärv eller utkontraktering och säkerställa att krav enligt författningen uppfylls av leverantören, utom i delar där kravet uppfylls av verksamhetsutövaren själv.

Detta bör justeras. En verksamhetsutövare kan inte alltid kräva att en global standardleverantör, molnleverantör eller komponentleverantör uppfyller samtliga svenska föreskriftskrav. Det relevanta är i stället att leverantören uppfyller de krav som är tillämpliga på leverantörens åtagande och den risk leveransen medför.

Föreslagen alternativ formulering av 4 kap. 1 § andra stycket:

Verksamhetsutövaren ska, i de delar leverantörens åtagande påverkar verksamhetsutövarens cybersäkerhet, ställa och följa upp krav som är lämpliga och proportionella i förhållande till leveransens art, omfattning och risk. Sådana krav kan uppfyllas genom avtalsvillkor, certifiering, tredjepartsintyg, revisionsrapport, teknisk dokumentation eller annan verifierbar dokumentation.

6. Synpunkter på utvalda bestämmelser

6.1 Ledningens utbildning, 2 kap.

SOFF och Teknikföretagen stödjer att ledningen ska ha tillräcklig kunskap för att kunna fastställa mål, bedöma säkerhetsåtgärder och övervaka genomförandet. Förslaget anger att ledningen ska ha kunskap och kompetens för att fastställa mål och inriktning, bedöma säkerhetsåtgärder och övervaka genomförandet.

MCF bör dock förtydliga att:

- utbildningen får anpassas efter ledningens roll och verksamhetens riskprofil,
- befintliga koncernutbildningar och styrelseutbildningar kan användas,
- dokumentation av genomförd utbildning bör vara tillräcklig som bevisning,
- utbildningskravet inte ska tolkas som ett krav på teknisk specialistkompetens hos ledningen.

Föreslagen komplettering i allmänt råd:

Utbildning kan genomföras genom intern eller extern utbildning, koncerngemensamt utbildningsprogram, styrelseutbildning eller motsvarande, förutsatt att utbildningen ger ledningen tillräcklig förståelse för verksamhetens cybersäkerhetsrisker, ansvarsfördelning, riskacceptans och uppföljning av säkerhetsåtgärder.

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

Förslaget använder begrepp som informationsägare, systemägare och samordnare. Detta är etablerade begrepp i många organisationer, men inte i alla. Privata företag kan använda

andra roller, exempelvis asset owner, service owner, product owner, process owner, business owner, control owner, CISO, CIO, OT security lead eller risk owner.

Kravet bör därför uttryckas funktionsbaserat och inte uppfattas som krav på viss organisationsmodell.

Föreslagen alternativ formulering av 3 kap. 5 §:

Verksamhetsutövaren ska utse roller, funktioner eller beslutsordningar som säkerställer ansvar för samordning av cybersäkerhetsarbetet, ansvar för krav på skydd av information samt ansvar för säkerhet i system och tjänster. Roller, funktioner eller beslutsordningar ska ha de befogenheter och resurser som krävs för sina uppgifter.

6.3 Personalsäkerhet, 3 kap. 9 §

Det är rimligt att verksamhetsutövare fastställer kontroller vid rekrytering och förändrad åtkomst. Kraven måste dock tillämpas i enlighet med arbetsrätt, dataskydd, diskrimineringsrätt och säkerhetsskyddslagstiftning. Förslaget bör undvika att skapa en förväntan om generella bakgrundskontroller för all personal.

Rekommendation: MCF bör förtydliga att kontroller ska vara lagliga, riskbaserade, proportionerliga och kopplade till den åtkomst personen ska ha.

6.4 Omvärldsbevakning, 3 kap. 10 §

Förslaget kräver att verksamhetsutövaren bedriver omvärldsbevakning och inhämtar information från bland annat leverantörer och NCSC samt ansluter sig till ANTS. Det anges också att verksamhetsutövaren ska identifiera och hantera behovet av att, om möjligt, ansluta sig till MISP-SE.

SOFF och Teknikföretagen stödjer kravet på omvärldsbevakning men anser att bindande krav på specifika nationella tjänster bör undvikas. Företag använder ofta flera internationella underrättelseflöden, branschspecifika ISAC:er, leverantörsflöden, CERT-tjänster, kommersiella threat intelligence-tjänster och koncerngemensamma SOC-funktioner.

Föreslagen alternativ formulering:

Verksamhetsutövaren ska säkerställa tillgång till relevant information om hot, sårbarheter, teknisk utveckling, rättsliga krav och tillgängligt stöd av betydelse för verksamhetens cybersäkerhet. Detta kan ske genom nationella eller internationella CSIRT-funktioner, leverantörer, branschorganisationer, informationsdelningsforum, kommersiella underrättelseflöden eller motsvarande.

ANTS och MISP-SE bör anges som goda exempel i allmänna råd, inte som generella bindande krav.

6.5 Riskhantering, 3 kap. 12–13 §§

Förslaget kräver riskvärdering för all informationsbehandling i system, enskilda system och segment i produktionsmiljön samt den digitala miljön i sin helhet. Detta är principiellt relevant men kan bli mycket omfattande i stora företag med tusentals system, molntjänster, mikrotjänster, fabriksutrustning, utvecklingsmiljöer och globala plattformar.

MCF bör tydliggöra att riskanalyser får göras på lämplig aggregeringsnivå, exempelvis per systemklass, tjänsteområde, plattform, process, produktionsanläggning, segment eller kontrollmiljö.

Föreslagen komplettering:

Riskvärdering får genomföras på den nivå som är lämplig med hänsyn till verksamhetens struktur, systemens likhet, beroenden, skyddsbehov och risk. Likartade system, tjänster eller informationsbehandlingar får grupperas, förutsatt att väsentliga skillnader i risk och skyddsbehov beaktas.

6.6 Utkontraktering och förvärv, 4 kap. 1–3 §§

Kraven på leverantörsutvärdering är viktiga men måste vara kommersiellt och praktiskt genomförbara. För internationella standardtjänster kan leverantörer ofta inte acceptera kundspecifika föreskriftskrav. Efterlevnad sker i stället genom standardiserade avtal, certifieringar, SOC-rapporter, tredjepartsgranskningar, teknisk dokumentation och standardiserade säkerhetsbilagor.

MCF bör också beakta att många försvarsindustriella leverantörskedjor omfattas av exportkontroll, sekretess, säkerhetsskyddsavtal och utländska myndighetskrav som kan begränsa vilken information som får delas.

6.7 Certifiering av system och tjänster, 4 kap. 2 §

Förslaget anger att verksamhetsutövaren ska identifiera och hantera behovet av att välja certifierade system och tjänster enligt europeiska cybersäkerhetscertifieringsordningar. I allmänna råd anges att sektorskritiska system bör vara certifierade enligt sådana ordningar.

Detta riskerar att bli svårt att tillämpa eftersom relevanta europeiska certifieringsordningar inte finns för alla produkter, tjänster eller systemtyper. För ex. OT, specialutvecklade system och internationella leveranser kan andra standarder och certifieringar vara mer relevanta.

Föreslagen alternativ formulering i allmänt råd:

Sektorskritiska system bör, när relevant och tillämplig certifieringsordning finns och när det är proportionerligt i förhållande till risk, vara certifierade enligt europeisk cybersäkerhetscertifieringsordning eller omfattas av annan likvärdig verifiering, exempelvis internationell standard, tredjepartsgranskning, säkerhetsgodkännande eller kund-/myndighetskrav.

6.8 Driftdokumentation och förteckningar, 4 kap. 7–9 §§

Förslaget innehåller omfattande allmänna råd om dokumentation av digital miljö, system, hårdvara, mjukvara, versioner, informationsflöden, kontaktuppgifter, konfigurationer och beroenden. Sådan dokumentation är viktig, men detaljeringsnivån måste vara riskbaserad.

I stora moln- och industrimiljöer kan krav på fullständig detaljförteckning över exempelvis hårdvaruversioner, MAC-adresser, IP-adresser och konfigurationer vara mycket resurskrävande och i vissa fall mindre relevant. Dokumentationen kan dessutom i sig vara mycket skyddsvärd.

Rekommendation: MCF bör ange att dokumentationen ska hållas på en detaljeringsnivå som behövs för riskhantering, incidenthantering, kontinuitet och tillsyn, och att verksamhetsutövaren får använda befintliga CMDB-, asset management-, OT asset inventory- och GRC-system.

6.9 Segmentering, 4 kap. 10–11 §§

Segmentering är en central säkerhetsåtgärd. Förslaget bör dock göras mer teknikneutralt. Krav på separata segment bör kunna uppfyllas genom fysisk separation, logisk separation, nätverkssegmentering, identitetsbaserad åtkomststyrning, mikrosegmentering, zero trust-arkitektur eller motsvarande.

Föreslagen komplettering:

Med segmentering avses fysisk, logisk eller annan teknisk separation som begränsar åtkomst, spridning och konsekvenser av incidenter. Val av segmenteringsmetod ska vara lämpligt och proportionellt i förhållande till systemens funktion, arkitektur och risk.

6.10 Behörighetshantering och flerfaktorsautentisering, 4 kap. 12–17 §§

SOFF och Teknikföretagen stödjer kraven på behörighetsstyrning, principen om minsta privilegium och flerfaktorsautentisering. Förslaget anger bland annat MFA för åtkomst till system i IT-segment som behandlar information med behov av utökat skydd, åtkomst via externt nätverk och systemadministrativ åtkomst.

MCF bör dock förtydliga att stark autentisering eller kompenserande kontroller kan användas när MFA inte är tekniskt möjlig eller lämplig, exempelvis i vissa OT-, äldre eller säkerhetskritiska system.

Föreslagen komplettering:

Om flerfaktorsautentisering inte är tekniskt möjlig eller lämplig med hänsyn till systemets funktion, säkerhet, tillgänglighet eller certifiering, får verksamhetsutövaren använda andra kompenserande kontroller som ger motsvarande riskreducerande effekt.

6.11 Säkerhetsloggning, realtidsövervakning och logganalys, 4 kap. 18–20 §§

Kraven är i huvudsak relevanta. MCF bör dock beakta dataskydd, arbetsrätt, företagshemligheter och säkerhetsskydd. Loggar kan innehålla personuppgifter, affärskritisk information och information som kan användas vid angrepp.

MCF bör därför ge vägledning om:

- rimliga loggningsnivåer,
- gallring och lagringstid,
- skydd av loggar,
- loggning i moln- och SaaS-miljöer,
- loggning i OT-miljöer,
- hur tillsyn kan ske utan att känsliga loggar sprids i onödan.

6.12 Robust och korrekt tid, 4 kap. 21 §

Förslaget anger att verksamhetsutövaren ska använda robust och korrekt tid som är översättningsbar till svensk UTC-tillämpning, UTC (SP), i produktionsmiljön. Det allmänna rådet pekar på Swedish Distributed Time Service.

För internationella företag är detta för specifikt. Det centrala bör vara att tiden är robust, korrekt och spårbar till UTC.

Föreslagen alternativ formulering:

Verksamhetsutövaren ska använda robust och korrekt tid som är spårbar till UTC eller på annat sätt möjliggör tillförlitlig korrelation av händelser vid incidenthantering, utredning och samverkan med andra organisationer.

6.13 Säkerhetstester och senaste version, 4 kap. 27 §

Förslaget anger att säkerhetstester ska användas för att kontrollera att systemen är uppdaterade till senaste version, publicerade sårbarheter är omhändertagna och valda konfigurationer har införts. Kravet på “senaste version” bör ändras. Senaste version är inte alltid den säkraste eller mest lämpliga versionen, särskilt inte i OT, säkerhetskritiska system, certifierade system eller system med höga tillgänglighetskrav.

Föreslagen alternativ formulering:

Säkerhetstester ska användas för att kontrollera att systemen är uppdaterade till en stödd och säkerhetsmässigt lämplig version, att relevanta publicerade sårbarheter har omhändertagits eller riskbehandlats, och att valda konfigurationer har införts.

6.14 Intrångsdetektering och intrångsskydd, 4 kap. 29 §

Förslaget kräver intrångsdetektering och intrångsskydd i produktionsmiljön. Kravet bör göras teknikneutralt och riskbaserat. I OT-miljöer kan aktiva intrångsskyddslösningar påverka driftsäkerhet och personsäkerhet. Passiv detektion, nätverksspegling och övervakning kan vara mer ändamålsenligt.

Föreslagen alternativ formulering:

Verksamhetsutövaren ska använda intrångsdetektering, intrångsskydd eller andra förebyggande och upptäckande kontroller som är lämpliga och proportionella i förhållande till produktionsmiljöns arkitektur, skyddsbehov, driftsäkerhet och risk.

6.15 Säkerhetsuppdateringar och 72-timmarsrådet, 4 kap. 31 §

Det allmänna rådet anger att arbetet med att införa en säkerhetsuppdatering bör påbörjas inom 72 timmar efter det att skyddande programvara har tillgängliggjorts. Detta kan vara rimligt för kritiska sårbarheter i vissa IT-miljöer men är inte generellt lämpligt för OT, försvarssystem, certifierade system eller system där uppdatering kräver test, leverantörsgodkännande eller driftstopp.

Föreslagen alternativ formulering i allmänt råd:

För kritiska sårbarheter bör verksamhetsutövaren utan onödigt dröjsmål, och normalt inom 72 timmar från att relevant säkerhetsuppdatering eller annan skyddsåtgärd finns tillgänglig, påbörja riskbedömning, prioritering och planering av åtgärd. Tidpunkt för införande bör fastställas utifrån risk, testbehov, driftsäkerhet och tillgängliga kompenserande kontroller.

6.16 Fysiska säkerhetsåtgärder, 5 kap.

Förslaget ställer krav på skydd av lokaler där information behandlas i system mot obehörigt tillträde genom tillträdesbegränsning och övervakning. MCF bör tydliggöra hur detta ska tillämpas vid distansarbete, hybridarbete, molntjänster, samlokaliserade kontor, co-working, kundmiljöer och internationella anläggningar.

Krav bör avse lokaler där system, utrustning eller administration av betydelse för cybersäkerheten finns, inte varje plats där en användare kan behandla information genom en bärbar dator.

Föreslagen förtydligande vägledning:

Krav på fysiskt skydd bör tillämpas riskbaserat och med beaktande av vilken utrustning, information och åtkomst som finns i lokalen. För distansarbete och mobilt arbete bör skyddet i första hand säkerställas genom tekniska och organisatoriska kontroller såsom kryptering, stark autentisering, enhetshantering, skärmlås, säker fjärråtkomst och riktlinjer för hantering av information.

6.17 Sektorsspecifika krav för offentlig förvaltning, 6 kap.

Kapitel 6 har rubriken “Offentlig förvaltning”, men bestämmelserna bör förtydligas så att det klart framgår att de endast gäller verksamhetsutövare inom sektorn offentlig förvaltning. Annars kan kravet på Rakel, SWEN och SGSI missförstås som ett generellt krav även för privata företag. Förslaget anger att verksamhetsutövare ska identifiera och hantera behovet av att, om möjligt, använda Rakel, SWEN och SGSI för kriskommunikation.

Föreslagen alternativ formulering:

Verksamhetsutövare inom sektorn offentlig förvaltning ska identifiera och hantera behovet av att, om möjligt och ändamålsenligt, använda Rakel, SWEN, SGSI eller motsvarande säkra kommunikationslösningar för kriskommunikation.

7. Behov av vägledning i stället för bindande krav

SOFF och Teknikföretagen bedömer att flera delar lämpar sig bättre för vägledning än bindande föreskrift. Detta gäller särskilt där tekniken utvecklas snabbt eller där olika sektorer har olika lösningar.

MCF bör prioritera vägledning om:

- tillämpning i koncerner och internationella företag,
- förhållandet till säkerhetsskyddslagstiftningen,
- riskbaserad dokumentationsnivå,
- leverantörskrav och avtalsklausuler,
- molntjänster och SaaS,
- OT- och industriella styrsystem,
- SME-anpassad efterlevnad,
- tillsynsbevisning och användning av certifieringar,
- incident- och sårbarhetsinformation som kan vara säkerhetskänslig,
- proportionalitet vid äldre system och tekniska begränsningar.

MCF:s konsekvensutredning anger att myndigheten avser att ta fram vägledning och erbjuda cybersäkerhetsrådgivning. Det är positivt, men vägledningen bör tas fram före eller i nära anslutning till ikraftträdandet och i dialog med näringslivet.

8. Ikraftträdande och övergångsbestämmelser

Förslaget saknar i remissversionen angiven tidpunkt för ikraftträdande. Det bör införas övergångsbestämmelser. Föreskrifterna innehåller krav som kräver förändringar i avtal, arkitektur, dokumentation, leverantörsstyrning, utbildning, loggning, incidentprocesser, fysisk säkerhet och tekniska miljöer. För vissa företag, särskilt inom försvar, OT och samhällsviktiga

aktörer, kan ändringar kräva kundgodkännande, säkerhetsskyddsbedömning, validering, certifiering, produktionsstopp eller upphandling.

SOFF och Teknikföretagen föreslår:

- minst 12 månaders övergångstid för organisatoriska krav,
- minst 18–24 månaders övergångstid för tekniska krav som kräver systemförändringar,
- särskild övergångstid för befintliga avtal och leverantörskedjor,
- möjlighet att visa efterlevnad genom riskbaserad åtgärdsplan under övergångsperioden,
- särskilda regler för äldre och OT-system där omedelbar teknisk anpassning inte är möjlig.

Föreslagen övergångsbestämmelse:

För krav som förutsätter ändring av befintliga system, tekniska miljöer, leverantörsavtal eller fysiska säkerhetsåtgärder får verksamhetsutövaren under en övergångsperiod visa efterlevnad genom dokumenterad riskbedömning och beslutad åtgärdsplan, under förutsättning att tillfälliga eller kompenserande säkerhetsåtgärder vidtas.

9. Konsekvensutredningen bör kompletteras

Konsekvensutredningen innehåller relevanta resonemang men bör kompletteras. MCF konstaterar att kostnader för cybersäkerhet kan vara svåra att separera från andra kostnader och att kostnader kan omfatta utrustning, programvara, datatrafikförbindelser, administration, personal, revisioner och utbildning. Det är korrekt, men det behövs mer detaljerad analys för näringslivet.

Kompletteringar bör särskilt avse:

- kostnader för SME-företag,
- kostnader för företag med OT och industriella produktionsmiljöer,
- effekter på försvarsföretags leveranskedjor,
- kostnader för omförhandling av avtal,
- effekter på internationella koncerner och global IT,
- effekter av krav på certifiering där relevanta certifieringsordningar saknas,
- administrativ börda vid dokumentations- och tillsynskrav,
- indirekta kostnader när stora verksamhetsutövare för vidare krav till mindre leverantörer,

- risk för fragmentering jämfört med andra medlemsstaters NIS2-implementering.

10. Avslutande synpunkter

SOFF och Teknikföretagen delar MCF:s målsättning att stärka cybersäkerheten i Sverige. Föreskrifterna har potential att ge verksamhetsutövare ett tydligare ramverk och stärka förmågan i samhällsviktiga verksamheter. För att regelverket ska få avsedd effekt behöver det dock vara rättssäkert, proportionerligt, teknikneutralt och praktiskt genomförbart. För detaljerade krav med specifika förslag på genomförande riskerar att bli obsoleta, men också att slå felaktigt mot vissa organisationer som hanterat hotbilden med andra lösningar. Kraven bör fokusera på vad som ska uppnås, inte hur det görs.

Särskilt för svenska försvarsföretag är det avgörande att regleringen stärker, och inte försvårar, förmågan att leverera säkra produkter och tjänster till totalförsvaret, svenska myndigheter, internationella partner och samhällsviktig verksamhet. Kraven bör därför harmoniseras övriga krav.

SOFF och Teknikföretagen står till förfogande för fortsatt dialog.