Sammandrag av remissvaren till Traficoms utkast till rekommendation till NIS-övervakande myndigheter för att övervaka åtgärder för riskhantering för cybersäkerhet enligt NIS 2-direktivet

Innehåll

1 Traficoms utkast till rekommendation

1.1 Utlåtanden om Traficoms utkast till rekommendation

Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom (nedan Traficom) bad de övervakande myndigheter om utlåtanden till utkast till rekommendation om åtgärder för riskhantering för cybersäkerhet enligt NIS 2-direktivet. Utkastet till rekommendationen var på remiss i tjänsten utlåtande.fi på finska i 8 veckor under tiden 5.4.2024–31.5.2024 (diarienummer: Traficom/18410/09.00.02/2023).

Sammanlagt mottogs 16 utlåtanden om utkastet till rekommendation.

Remissinstanserna bestod av övervakande myndigheter och aktörer som omfattas av lagstiftningens tillämpningsområde samt aktörer utanför lagstiftningens tillämpningsområde. Följande instanser yttrade sig om utkastet till rekommendation: Byggnadsindustrin RT rf, Finlands Konfessionella Lutherska kyrka, Jord- och skogsbruksministeriets informations- och forskningssektor, Finnish Information Security Cluster - Kyberala ry, FiCom rf, Finlands Vattenverksförening rf, Rederierna i Finland rf, Finlands Näringsliv EK, Tillstånds- och tillsynsverket för social- och hälsovården Valvira, Finlands Kommunförbund rf, Livsmedelsverket, Energiindustrin rf, Säkerhets- och utvecklingscentret för läkemedelsområdet Fimea och Informationshanteringsnämnden. Dessutom lämnade Verizon in ett allmänt ställningstagande om ett enhetligt genomförande av NIS 2-direktivet i medlemsländerna. Säkerhets- och kemikalieverket Tukes hade inget att uttala sig om i ärendet.

1.2 Sammanfattning av utlåtandena

Enligt remissvaren anses utkastet till rekommendation allmänt taget fungera som stöd för de övervakande myndigheterna och aktörerna. Rekommendationen upplevs konkretisera genomförandet av de riskhanteringsskyldigheter som lagstiftningen medför på praktisk nivå. Innehållet i utkastet till rekommendation anses i princip vara heltäckande och strukturen tydlig, eftersom den följer strukturen för motsvarande delar i regeringens proposition om en cybersäkerhetslag. Tabelluppställningen som hade valts som presentationssätt upplevs förbättra begripligheten. Det att varje enskild rekommendationsåtgärd är motiverad och innehåller en tydlig hänvisning till referensramarna ansågs som en bra lösning.

Å andra sidan upplever man det som problematiskt att varje riskhanteringsåtgärd granskades som en enskild åtgärd separat från de övriga kraven, eftersom det kan leda till att hanteringen av varje risk inleds med samma intensitet. Dessutom önskas det att den inbördes

kompensationen mellan åtgärderna i rekommendationen beaktas bättre. Rekommendationen upplevs också som lång och därför önskas ett sammandrag av hanteringsåtgärderna.

I rekommendationen har man medvetet strävat efter att presentera varje riskhanteringsåtgärd som en egen självständig helhet och beskriva innehållet i hanteringsåtgärden. Detta har lett till att exemplen delvis överlappar varandra. Motiveringstexten för varje enskild riskhanteringsåtgärd som presenteras i rekommendationen anses fungera som ett sammandrag.

Rekommendationens terminologi har förtydligats och hänvisningarna i rekommendationen preciserats enligt responsen. Rekommendationens inledning har kompletterats och preciserats till den del responsen gällt proportionalitetsprincipen, ledningens ansvar, riskbasering och rekommendationens förhållande till eventuella preciserande tekniska föreskrifter som myndigheterna utfärdar. Dessutom har läsanvisningen kompletterats genom att precisera definitionen av aktörer på högre cyberrisknivå.

Motsvarigheten mellan riskhanteringsåtgärderna i rekommendationen och de referensramar (standarder och bedömningskriterier) som tillämpades i rekommendationen upplevs som problematisk. Ett korshänvisningsdokument som utarbetats av Traficom har utifrån responsen fogats till rekommendationen och rekommendationens inledning har kompletterats för att undvika eventuella missförstånd om att det skulle vara fråga om harmoniserade standarder som direkt uppfyller lagens krav.

Det gavs både allmänna utlåtanden och åtgärdsspecifika utlåtanden om riskhanteringsåtgärderna i rekommendationen. Rekommendationen har i första hand uppdaterats så att den motsvarar den ändrade regeringspropositionen om cybersäkerhetslagen och därefter har remissvaren om cybersäkerhetsåtgärderna från remissrundan om möjligt beaktats genom ändringar eller preciseringar av rekommendationen. Observationer om branschspecifika standarder och anvisningar har fogats till rekommendationen i enlighet med förslagen.

I samband med remissbehandlingen inkom dessutom respons som direkt anknyter till övervakningen av och resurser för riskhanteringsåtgärderna men denna respons kunde inte beaktas i rekommendationen. Respons om övervakningen och aktörernas resurser förmedlas i mån av möjlighet till de övervakande myndigheterna som en del av Traficoms kommande uppgift som gemensam kontaktpunkt enligt NIS 2-direktivet.

Enligt remissvaren anses det vara problematiskt att remissförfarandet för utkastet till rekommendationen ordnades innan riksdagsbehandlingen av cybersäkerhetslagen avslutats, vilket även Traficom känt till. Traficom skickade utkastet till rekommendation på remiss trots den utmanande tidpunkten för remissförfarandet, eftersom detta ansågs konkretisera genomförandet av riskhanteringsåtgärderna även i sin halvfärdiga form och vara till hjälp särskilt för de nya övervakande myndigheterna och aktörerna inom lagstiftningens tillämpningsområde.

2 Allmänna utlåtanden om utkastet till rekommendation

2.1 Rekommendationen som stöd för de övervakande myndigheterna och aktörerna

Rekommendationen anses fungera som en bra utgångspunkt för övervakningen som helhet och stödja de övervakande myndigheterna i att enhetligt tillämpa den nationella regleringen över branschgränserna. Utkastet till rekommendation förenhetligar övervakningspraxisen inom olika sektorer men ger trots det den övervakande myndigheten möjlighet till prövning från fall till fall (Byggnadsindustrin RT rf, Jord- och skogsbruksministeriet, Finnish Information Security Cluster

(FISC) - Kyberala ry, Finlands Näringsliv EK, Tillstånds- och tillsynsverket för social- och hälsovården Valvira, Finlands Kommunförbund rf, Säkerhets- och utvecklingscentret för läkemedelsområdet Fimea, FiCom rf).

Rekommendationen anses på ett allmänt plan vara nödvändig eftersom genomförandeexemplen i utkastet till rekommendation omfattar riskhanteringsåtgärderna i NIS 2-direktivet och de upplevs styra, stöda och förenhetliga en proportionell bedömning och planering av aktörernas egen riskhantering samt genomförandet av riskhanteringen (Byggnadsindustrin RT rf, Jord- och skogsbruksministeriet, FiCom rf, Finlands Vattenverksförening rf, Rederierna i Finland rf, Finlands Kommunförbund rf).

Att de genomförande- och verifieringsmetoder som ingår i rekommendationen utgör, beroende på aktör och bransch, varierande exempel på vad kraven innebär i praktiken och vad som ska uppmärksammas vid övervakningen av hur kraven iakttas anses vara positivt (Informationshanteringsnämnden, FiCom rf).

Rekommendationen upplevs som ett välkommet sätt att optimera styrningen, eftersom riskhanteringsåtgärderna som den omfattar gäller den osäkerhet i övervakningens förutsägbarhet och konsekvens som decentraliseringen av myndighetstillsynen medför (Finnish Information Security Cluster (FISC) - Kyberala ry).

Det anses att de goda praxis som ingår i rekommendationen också kan utnyttjas för styrning av sådana aktörer som inte direkt omfattas av tillämpningsområdet för lagstiftningen om genomförandet av NIS 2-direktivet (Säkerhets- och utvecklingscentret för läkemedelsområdet Fimea). Aktörerna anses i tillämpliga delar kunna utnyttja rekommendationen även i bedömningen av de egna tjänsteleverantörerna och -avtalen (Finlands Kommunförbund rf).

Det upplevs också som positivt att många samarbetspartner som tillhandahåller externa tjänster för aktörerna också omfattas av lagstiftningens tillämpningsområde (Säkerhets- och utvecklingscentret för läkemedelsområdet Fimea).

2.2 Rekommendationens innehåll och tydlig struktur

Utkastet till rekommendationen upplevs allmänt taget som heltäckande, tydligt, mångsidigt och praktiskt (Finlands Kommunförbund rf, Säkerhets- och utvecklingscentret för läkemedelsområdet Fimea, Jord- och skogsbruksministeriet). Det anses positivt att genomförande- och verifieringsexemplen i utkastet till rekommendation följer NIS 2-direktivets struktur och att de presenteras i samma ordning som i förslaget till cybersäkerhetslag (Jord- och skogsbruksministeriet, Livsmedelsverket, FiCom rf).

Tabelluppställningen som valts som presentationssätt för rekommendationens innehåll upplevs förbättra utkastets begriplighet (FiCom rf). Även indelningen av presentationssättet i exempel på genomförande, verifiering, motivering och källor samt utvidgade anvisningar upplevs som bra (Rederierna i Finland rf). Med tanke på både övervakningen och aktörerna anses det vara bra att enskilda rekommendationer är motiverade och att det för varje åtgärd hänvisas tydligt till underliggande källor, till exempel standarder (Tillstånds- och tillsynsverket för social- och hälsovården Valvira).

När det gäller riskhanteringsmetoder som aktörerna redan identifierat och genomfört anses det också viktigt att det i rekommendationen finns innehåll från den nationellt kända Cybermätaren och hänvisningar till det (Näringslivets centralförbund EK). Även hänvisningarna till andra referensramar (standarder) upplevs som nyttiga (Finnish Information Security Cluster (FISC) - Kyberala ry).

2.3 Detaljerade riskhanteringsåtgärder är problematiska – partiella preciseringar i rekommendationen

I remissvaren kritiserar man också rekommendationens struktur för det att varje enskilt krav i 9 § i cybersäkerhetslagen granskas separat från de andra kraven i rekommendationen. Man önskade att riskhanteringsåtgärderna i motsats till detta bedöms som en helhet där man beaktar en eventuell kompensation mellan åtgärderna på basis av de bedömda riskerna (Näringslivets centralförbund EK). I rekommendationen har man medvetet strävat efter att presentera varje riskhanteringsåtgärd som en egen självständig helhet och beskriva innehållet i hanteringsåtgärden. Detta har lett till att exemplen delvis överlappar varandra.

Rekommendationens stora antal sidor upplevs försämra tillägnandet av innehållet och därmed styrningens effektivitet. På grund av detta önskar man ett sammandrag eller en sammanfattning av rekommendationerna i början av dokumentet för att underlätta tillägnandet (Informationshanteringsnämnden). Motiveringstexten för varje enskild riskhanteringsåtgärd som presenteras i rekommendationen anses fungera som ett sammandrag.

Respons gavs också om bristerna i urvalet av riskhanteringsmetoder i utkastet till rekommendation till den del det inte är möjligt eller förnuftigt att minimera sannolikheten för eller effekterna av alla risker. Däremot kan en identifierad risk godkännas av motiverade skäl. Rekommendationen ger en felaktig bild av att alla risker bör hanteras med samma intensitet (Näringslivets centralförbund EK). En allt för detaljerad reglering innebär en systematisk risk och en risk för att aktörernas begränsade resurser riktas till myndighetsrapportering (Energiindustrin rf). Allmän riskhantering och godkännande av kvarstående risk behandlas separat i avsnitt 1.5 i rekommendationen. Genom att precisera rekommendationens inledning i fråga om riskbedömning, övervägd riskhantering och proportionalitetsprincipen anses responsen ha beaktats.

2.4 Terminologin som används i rekommendationen förtydligades och hänvisningarna preciserades

I remissvaren uppmärksammades att namnet på den författning som avses i utkastet till rekommendation ska uppdateras så att det motsvarar regeringens proposition om cybersäkerhetslagen (RP 57/2024 rd) (Finnish Information Security Cluster (FISC) - Kyberala ry, Finlands Näringsliv EK).

Dessutom beaktades de nya myndigheterna och aktörerna som kommer att omfattas av lagstiftningens tillämpningsområde vad gäller den för dem nya tekniska terminologin om informationssäkerhet genom att definitionerna i rekommendationen utökades med vissa termer som upplevs som svåra (bl.a. konfigurering, härdning och principen om noll förtroende) (Livsmedelsverket).

På grund av responsen om varierande definitioner av termerna, oenhetlighet eller avsaknaden av termer beslöt man att till rekommendationen också foga en precisering om att ett begrepp definieras i rekommendationen endast om det inte redan definierats i cybersäkerhetslagen (Näringslivets centralförbund EK, Energiindustrin rf, Finnish Information Security Cluster (FISC) - Kyberala ry).

Dessutom uppmärksammades att rekommendationen innehöll en hänvisning till en delvis föråldrad anvisning (anvisning om säkerhetskritiska upphandlingar VM2019:7). Hänvisningen har uppdaterats (rekommendation om informationssäkerhet vid upphandling VM2023:57).

Observationer om branschspecifika standarder och anvisningar framfördes förutom av Informationshanteringsnämnden även av Byggnadsindustriförbundet RT rf och Finlands Konfessionella Lutherska kyrka och rekommendationen ändrades enligt förslagen.

2.5 Rekommendationens inledning kompletterades och preciserades – riskbasering och rekommendationens förhållande till föreskrifter

På basis av remissvaren kunde man allmänt taget dra slutsatsen att rekommendationen kan behandlas som ett dokument separat från lagstiftningen och dess motiveringar och inte som ett dokument som kompletterar lagstiftningshelheten. Det framfördes särskilt att det inte är nödvändigt eller resurseffektivt att förutsätta att alla aktörer vidtar alla åtgärder som presenteras i utkastet eller att de införs i all verksamhet (Näringslivets centralförbund EK, Finlands Vattenverksförening rf). I responsen önskade man också att rekommendationen tydligare skiljer åt vad som är lagstadgade krav och vad som är motiveringstext (Energiindustrin rf).

Man beslöt att i rekommendationens inledning beslöt precisera att rekommendationen endast har skapats för att konkretisera alternativ för verifiering av de åtgärder som avses i 9 § i cybersäkerhetslagen och 18 c § 1–12 punkterna i informationshanteringslagen och som beskrivs närmare i motiveringarna till dessa. Dessutom preciserades att tillvägagångssättet även bygger på andra bestämmelser som nära anknyter till riskhanteringsåtgärderna i cybersäkerhets- och informationshanteringslagarna, till exempel den riskbedömning som anknyter till respektive bransch samt aktörens övervägda riskhantering som beaktar proportionalitetsprincipen och bestämmelserna om ledningens ansvar.

Enligt remissvaren är tanken om att rekommendationen utvidgar de lagstadgade kraven i oroväckande mån (Näringslivets centralförbund EK, Finnish Information Security Cluster (FISC) - Kyberala ry, Energiindustrin rf). Förhållandet mellan rekommendationen som var på remiss och eventuella tekniska föreskrifter utfärdade av de övervakande myndigheterna upplevs också som oklart (Näringslivets centralförbund EK, Energiindustrin rf). I samband med förankringen av rekommendationen önskar man att det lyfts fram att rekommendationen inte är bindande myndigheter eller aktörer (Finlands Vattenverksförening rf).

Utifrån responsen har rekommendationens inledning preciserats till den del som man i texten behandlar rekommendationens karaktär endast som ett styrande och assisterande dokument och rekommendationens innehåll i förhållande till eventuella preciserande tekniska föreskrifter som utfärdats av de övervakande myndigheterna.

2.6 Rekommendationens läsanvisning kompletterades och preciserades – aktörer på högre cyberrisknivå

För att skapa enhetlig övervakningspraxis önskade man att rekommendationen tar ställning till vilka aktörer som förväntas ha en högre mognadsnivå (Jord- och skogsbruksministeriet). Rekommendationens inledning har preciserats utifrån responsen.

Användningen av de referensramar som presenteras i rekommendationen är inte förpliktande och användningen av dem är inte allmänt eller branschspecifikt begränsad. Således beaktades inte i remissvaren begäran om att precisera på vilken typ av verksamhet bedömningskriterierna borde tillämpas (Näringslivets centralförbund EK).

2.7 Utmaningar med riskhanteringsåtgärdernas och referensramarnas överensstämmelse – publicering av korshänvisningsdokument som bilaga till rekommendationen

Enligt remissvaren upplever aktörerna det som problematiskt att man av rekommendationen inte direkt kan sluta sig till om de punkter som anknyter till kraven i de standarder som det hänvisas till i rekommendationen är tillräckliga för att tillgodose kraven i cybersäkerhetslagen eller om det krävs ytterligare åtgärder (Finnish Information Security Cluster (FISC) - Kyberala ry). Därför har man bedömt att det mervärde som utkastet till rekommendation medför blir mindre än planerat (Finlands Konfessionella Lutherska kyrka).

Utnyttjandet av andra myndigheters rekommendationer ansågs främja syftet med informationshanteringslagen, men samtidigt framfördes att bland annat kriterierna i Julkri-rekommendationen inte nödvändigtvis i sig är ett tillräckligt sätt att verifiera de skyldigheter som föreslås i lagen. Således föreslogs ytterligare hänvisningar till befintliga bestämmelser om informationssäkerhet och informationshantering i informationshanteringslagen, med vilka man kan skapa tillräcklig omfattning med tanke på verifieringen av överensstämmelse med kraven (Informationshanteringsnämnden). Traficom beaktar i rekommendationen hänvisningarna till nämndens befintliga rekommendationer men inte direkta hänvisningar till de befintliga paragraferna om informationshantering och informationssäkerhet i informationshanteringslagen.

Man önskade att motsvarigheter mellan att uppfylla korshänvisningarna, dvs. referensramarna, och att tillgodose överensstämmelse med kraven i cybersäkerhetslagen, läggs till i rekommendationen som stöd för aktörerna och de övervakande myndigheterna (Finnish Information Security Cluster (FISC) - Kyberala ry, Livsmedelsverket, Finlands Konfessionella Lutherska kyrka). Utifrån responsen fogades Traficoms korshänvisningsdokument om referensramarna som bilaga till rekommendationen, men för att undvika missförstånd fogades en precisering till rekommendationens läsanvisning om att det inte är fråga om en harmoniserad standard som endast uppfyller kraven i cybersäkerhetslagen.

2.8 Respons på övervakningen – inga ändringar i rekommendationen

Man önskade stöd av myndigheterna för att säkerställa att riskhanteringsåtgärderna de facto leder till att de digitala riskerna minskar i stället för att verksamheten utgör en administrativ börda för aktörerna. Det centrala är att lagstiftningen tillämpas så enhetligt som möjligt mellan medlemsstaterna samt på motsvarande sätt på nationell nivå inom olika sektorer (Finnish Information Security Cluster (FISC) - Kyberala ry).

Ett önskemål var också att de övervakande myndigheterna bedriver ett förutseende, flexibelt och långsiktigt samarbete i växelverkan med aktörerna inom den egna branschen i form av handledning, rådgivning och stöd för att fastställa ramvillkoren för verksamheten samt för att säkerställa att aktörerna inte överdimensionerar riskhanteringsåtgärderna. Även samordningen och samarbetet mellan de övervakande myndigheterna bör kunna ordnas på nationell nivå så att övervakningen är av jämn kvalitet mellan olika branscher (Finlands Kommunförbund rf).

I remissvaren framfördes också att den tvingande reglering som fastställts för aktörerna inte får hindra att kostnaderna för genomförandet av lagstiftningen täcks på bekostnad av den övriga verksamheten (Energiindustrin rf).

En utmaning i den offentliga förvaltningens tillsynsverksamhet ansågs vara hur förenligt det nya 4 a kap. i informationshanteringslagen om cybersäkerhetsskyldigheter och övervakningen av dem är med de befintliga bestämmelserna om informationssäkerhet och informationshantering i informationshanteringslagen. Även samarbetet mellan den myndighet som övervakar den offentliga förvaltningen och Informationshanteringsnämnden ansågs betydelsefullt för att förenhetliga anvisningarna och rekommendationerna och effektivisera övervakningen (Informationshanteringsnämnden).

I remissvaren föreslogs också att man bör överväga att lägga till nationellt enhetliga elektroniska mallblanketter (t.ex. mallar till inspektionsprotokoll eller frågebatterier) som bilaga till rekommendationen, som kan användas av de sektorspecifika tillsynsmyndigheterna vid tillämpningen av cybersäkerhetslagen och rekommendationen (Tillstånds- och tillsynsverket för social- och hälsovården Valvira).

I remissvaren begärdes en precisering av riskhanteringsåtgärden som gäller ledningens förtrogenhet genom att definiera begreppet ledning för multinationell koncern. Enligt responsen bör man ge definitionsmässiga anvisningar för att det ska vara klart i vilka fall koncernledningen ska vara informerad om de nationella kraven (FiCom rf).

Responsen innehöll en begäran om att man ska fästa uppmärksamhet vid att definitionen av NIS 2-tillämpningsområdet som en kombination av definitionerna för bransch, storlek och oberoende av storlek de facto upplevs som utmanande. Även om utkastet till rekommendation inte gäller definitionen av lagstiftningens tillämpningsområde som sådan, önskade man att det i övervakningen och tolkningen av riskhanteringsåtgärderna vore möjligt att fästa uppmärksamhet vid aktörens uppskattade faktiska risk. Man önskade att man i tillsynsverksamheten skulle beakta förståelsen för riskerna, så att de riskhanteringsmetoder som förutsätts de facto minskar riskens sannolikhet och inverkan (Näringslivets centralförbund EK).

I remissvaren framfördes vikten av att övervakningen tillämpas enligt aktörens storlek och verksamhet samt med beaktande av aktörernas olika risker och behov av att använda olika riskhanteringsmodeller. Den övervakande myndigheten bör förtydliga närmare vad som ingår i riskidentifieringen, hotanalysen och verksamhetsmodellen för riskhantering. Med tanke på ett eventuellt obligatoriskt säkerhetsledningssystem och de befintliga internationella cybersäkerhetskraven är det viktigt att man i aktörernas verksamhetsmodell för cybersäkerhet också kan utnyttja befintliga system och arrangemang för att undvika överlappningar (Rederierna i Finland rf).

Särskilt med tanke på övervakningen önskades tid för att införa riskhanteringsåtgärder samt växelverkande styrning och stöd, särskilt för aktörer som arbetar med begränsade ekonomiska resurser, personalresurser och kompetensresurser (Finlands Vattenverksförening rf).

Ovan nämnda respons i direkt anslutning till övervakningen av riskhanteringsåtgärderna kunde inte beaktas i rekommendationen, men den har om möjligt förmedlats till de övervakande myndigheterna som en del av Traficoms kommande uppgift som gemensam kontaktpunkt enligt NIS 2-direktivet.

2.9 Resurser som en utmaning för övervakningen och aktörerna – inga ändringar i rekommendationen

Av remissvaren framgår att aktörerna upplever att till och med minimigenomförandet av NIS 2-direktivet och cybersäkerhetslagen är en utmaning med tanke på den rådande situationen för de offentliga finanserna (Jord- och skogsbruksministeriet). På aktörernas vägnar framfördes också att NIS 2-aktörerna omfattar aktörer med mycket olika resurser som i och med den nya lagstiftningen omfattas av ytterligare krav (Finlands Vattenverksförening rf).

Enligt remissvaren torde säkerställandet av överensstämmelse med kraven kräva betydande uppdateringar av cybersäkerhetslösningarna och verksamhetsmodellerna för största delen av de organisationer som omfattas av lagstiftningens tillämpningsområde. Därför behövs mer kompetens och resurser än i nuläget samt att det byggs upp en ny säkerhetskultur (Finlands Kommunförbund rf).

I allmänhet väcker den rikliga och delvis överlappande lagstiftningen om cybersäkerhet frågor hos aktörerna om huruvida cybersäkerheten de facto förbättras samt oro för kostnadseffektiviteten i verksamheten (Energiindustrin rf).

Ovan nämnda respons i direkt anslutning till resurserna kunde inte beaktas i rekommendationen, men aktörernas respons har om möjligt förmedlats till de övervakande myndigheterna som en del av Traficoms kommande uppgift som gemensam kontaktpunkt enligt NIS 2-direktivet.

2.10 Allmänt ställningstagande om ett enhetligt genomförande av NIS 2-direktivet

Utöver vad som anförs ovan lämnade Verizon in ett allmänt ställningstagande om ett enhetligt genomförande av NIS 2-direktivet som beaktar andra bestämmelser om cybersäkerhet i

medlemsländerna. Ställningstagandet innehöll en önskan om ett kostnadseffektivt, teknikneutralt genomförande som beaktar de allmänna internationella standarderna och ett riskbaserat tillvägagångssätt enligt artikel 21 om riskhanteringsåtgärder för cybersäkerhet. Dessa har redan beaktats som grundläggande principer i det utkast till rekommendation som varit på remiss.

3 Utlåtanden om riskhanteringsåtgärder för cybersäkerhet

3.1 Riktlinjer för åtgärder för hantering av cybersäkerhetsrisker och bedömning av effektiviteten av riskhanteringsåtgärder

De tillägg som Kyberala rf föreslagit om att förtydliga den mer omfattande logiken i verksamhetsmodellen för riskhanteringen har gjorts i rekommendationen. Byggnadsindustriförbundet RT rf framförde en anmärkning om husteknikens betydelse i anknytning till den fysiska miljön och dess nödvändiga resurser och lokalsäkerheten. Förslaget beaktades i den 12:e åtgärden som behandlar den fysiska säkerheten närmare.

Finlands Näringsliv EK gav ett utlåtande om metodurvalet för riskhanteringen och lyfte framaccepterande av risk och uppföljning av risker med beaktande av riskhelheten inom ramen för den egna riskbärkraften. Innehållet i avsnittet i fråga motsvarar motiveringstexten i lagen och därför ansågs det att texten i rekommendationen inte kan ändras. Responsen övervägdes dock i samband med i avsnitt 1.5 (riskhantering) i rekommendationen, där man redan beaktar möjligheten att acceptera risken.

3.2 Riktlinjer som gäller säkerheten i kommunikationsnät och informationssystem

FiCom rf:s respons på säkerhetsprinciperna har beaktats och de begärda ändringarna införts i verifieringsmetoderna.

3.3 Säkerheten vid förvärv, utveckling och underhåll av kommunikationsnät och informationssystem samt behövliga förfaranden för hantering och offentliggörande av sårbarheter

FiCom rf påpekade om avsnitt 3.2 (säkerheten hos föremålet för upphandlingen) att livscykelhanteringen också är beroende av livscykeln hos teknik som skaffats tidigare, som kan vara anmärkningsvärt lång. Dessutom påpekade FiCom ry om punkt 3.8 utmaningarna med att begränsa den tidsbaserade åtkomsten. Man har varit medveten om båda utmaningarna när rekommendationen utarbetades. Det var inte motiverat att göra de önskade ändringarna i rekommendationen. De genomföranden som presenteras i rekommendationen är exempel och har utarbetats så att de lämpar sig för olika branscher och aktörer av olika storlek.

Verifieringsmetoden i avsnitt 3.9 har preciserats utifrån FiCom rf:s anmärkning om avtalsmässiga begränsningar för penetrationstestning av molntjänster.

3.4 Den övergripande kvaliteten och resiliensen i leveranskedjan för leverantörers produkter och tjänsteleverantörers tjänster och de åtgärder för hantering av cybersäkerhetsrisker som är inbyggda i dem samt tillvägagångssätt för cybersäkerhet hos leverantörer och tjänsteleverantörer

-

3.5 Tillgångsförvaltning och identifiering av funktioner som är viktiga med tanke på dess säkerhet

Enligt Byggnadsindustrin RT rf:s utlåtande avses med egendom också hyrda lokaler, programvara och andra resurser som omfattas av egendomsförvaltningen och som aktören har i sin besittning eller innehar. Rekommendationen har kompletterats utifrån Byggnadsindustrin RT rf:s observationer.

3.6 Personalsäkerhet och utbildning i cybersäkerhet

Finlands Kommunförbund rf uttalade sig om de förfaranden för granskning av personers bakgrund, som kommunerna eller kommunernas energi-, vatten- och avfallshanteringsorganisationer inte har tillgång till i någon större utsträckning och påpekade att det här är en eventuell flaskhals i genomförandet. Finlands Kommunförbund rf:s anmärkning bedömdes inte orsaka något behov av uppdatering, eftersom den övervakande myndigheten har befogenhet att bedöma tillämpningen av hanteringsmetoden i fråga.

FiCom rf framställde en begäran om precisering av avsnitt 6.6 om ledningens förtrogenhet i fråga om hur ledning definieras i en multinationell koncern. Enligt FiCom rf bör man ge definitionsmässiga anvisningar för att det ska vara klart när koncernledningen ska vara informerad om de nationella kraven. FiCom rf:s begäran har lyfts fram i kommentarer om övervakningen som man om möjligt strävar efter att förmedla till den övervakande myndigheten.

3.7 Åtkomsthantering och autentisering

-

3.8 Riktlinjer och förfaranden som gäller användningen av krypteringsmetoder samt vid behov åtgärder för användningen av skyddad elektronisk kommunikation

-

3.9 Upptäckande och hantering av incidenter i syfte att återställa och upprätthålla säkerheten och driftsäkerheten

FiCom rf framförde respons om att precisera definitionen av incidenter. I texten till utkastet till rekommendation som skickats på remiss är inte informationssäkerhetsincidenter tydligt åtskilda från incidenter som har konsekvenser för informationssäkerheten. Definitionen har betydelse vid utvecklingen av processerna för behandling av incidenter samt vid bedömningen av praktiskt taget alla underpunkter i avsnittet. Den definition som används i utkastet till rekommendation kommer från cybersäkerhetslagen. Definitionerna i det inledande stycket i utkastet till rekommendation kommer att preciseras till denna del och samtidigt stryks hänvisningarna till cybersäkerhetslagen för att undvika överlappning.

Utifrån FiCom rf:s respons har formuleringen av tidsdefinitionen i verifieringsmetoderna i avsnitt 9.3 (registrering och upptäckande av händelser) ändrats, men det nuvarande uttrycket anses vara motiverat i exemplet på genomförande, eftersom det är konkret och ett exempel.

3.10 Säkerhetskopiering, återhämtningsplanering, krishantering och annan hantering av verksamhetens kontinuitet och vid behov användning av skyddade reservkommunikationssystem

Kyberala ry gav respons på tydligheten och strukturering i avsnitt 10.2 (säkerhetskopior och reservsystem) samt avsnitt 10.4 (reservkommunikationssystem). Man önskade att åtgärderna skulle vara logiskt strukturerade och tydligt separerade. Utifrån responsen har i synnerhet

genomförandeexemplet i avsnitt 10.2 kompletterats. Dessutom har termerna ”reservsystem” och ”säkerhetskopia” införts i definitionerna.

Kyberala ry påpekade att rekommendationen på flera ställen i avsnitt 10 innehåller upprepningar, vilket ställvis gör dokumentet onödigt långt. Man har beslutat att inte ändra rekommendationens nuvarande formulering. Överlappningen är avsiktlig så att varje tabell är en egen enskild helhet.

3.11 Grundläggande informationssäkerhetsrutiner för att säkerställa säkerheten i datakommunikationen, maskinvaran, programvaran och datamaterialet

Kyberala ry påpekade att samma sak behandlas på flera ställen i rekommendationen och påpekade att detta stör läsningen. Som exempel nämndes avsnitten 10.3 och 11.11 som behandlar säkerhetskopiors betydelse och testning. Av rekommendationen bör tydligt framgå vad som ska göras mer i avsnitt 10.3 utöver åtgärden på basnivå i avsnitt 11.11. Till rekommendationens grundläggande informationssäkerhetsrutiner har fogats hänvisningar till den egentliga åtgärden. I underpunkterna i avsnitt 11 har sådana exempel på genomförande som tydligt överlappar med exemplen i andra avsnitt slopats.

3.12 Åtgärder för att skydda kommunikationsnätens och informationssystemens fysiska miljö och säkerställa säkerheten i lokalerna samt nödvändiga resurser

Byggnadsindustriförbundet RT rf påpekade att man i avsnitt 12 och dess underpunkter och i andra motsvarande sammanhang som behandlas senare bör nämna att åtgärderna utöver kommunikationsnäten och informationssystemen samt deras fysiska miljö även omfattar lokalsäkerhet samt system och tjänster för nödvändiga resurser, för vilka den digitala säkerhetsnivån DT2 som presenteras i anvisningarna för byggnaders digitala säkerhet motsvarar basnivån för lokalfastigheter. DT1 lämpar sig för bostadsfastigheter och andra objekt med låg risk. Anvisningarna i fråga har lagts till bland rekommendationens hänvisningar, men genomförandeexemplet har inte preciserats till denna del. Avsnitten om den fysiska miljön och dess nödvändiga resurser samt lokalsäkerheten har setts över så att även husteknikens betydelse beaktas i rekommendationen.

Till hänvisningarna i avsnitt 12 i rekommendationen har fogats de anvisningar för byggnaders digitala säkerhet som Byggnadsindustriförbundet RT rf lagt fram.