Utfärdad:	Träder i kraft:	Giltighetstid:
30.11.2020	30.11.2020	tills vidare

Anvisningen grundar sig på följande lagstiftning:
Lagen om tjänster inom elektronisk kommunikation (917/2014) 243, 247 och 272 §

Ändringsuppgifter:
Ersätter Kommunikationsverkets rekommendation 312 A/2018 S

INFORMATIONSSÄKERHETSBASERAD FILTRERING AV TRAFIK TILL VISSA KOMMUNIKATIONSPORTAR I TELEFÖRETAGENS NÄT

Transport- och kommunikationsverkets rekommendation 312/2020 S

Innehåll

1 Inledning

1.1 Bakgrund och syfte

För internettrafik gäller enligt lag (se kap. 3) en s.k. nätneutralitetsprincip. Det betyder att i olika internettjänster ska all trafik behandlas likvärdigt, utan diskriminering, begränsningar eller störanden, och oberoende av sändare eller mottagare, innehåll, applikation, tjänst eller terminalutrustning.

I lagen förutsätts samtidigt även att teleföretagen sörjer för informationssäkerheten i sina nät och tjänster samt anges vissa situationer och villkor som möjliggör undantag från nätneutralitetsprincipen: att sörja för informationssäkerheten är en sådan grund. Ett teleföretag kan tillfälligt förhindra eller begränsa trafik till en viss port i den mån det är nödvändigt för att sörja för informationssäkerheten och så länge det är nödvändigt. Det väsentliga vid sådant förhindrande är att:

1. filtreringsåtgärder står i rätt proportion till det hot som avvärjs,
2. åtgärderna utförs utan att yttrandefriheten, skyddet av konfidentiella meddelanden eller integritetsskyddet begränsas mer än vad som är nödvändigt och
3. åtgärderna avslutas om det inte längre finns förutsättningar för att vidta dem.

I praktiken betyder det att vid övervägande av filtrering ska man alltid bedöma huruvida filtrering är nödvändig och om den är, hur länge. Filtreringsåtgärder som vidtas med tanke på informationssäkerheten är i princip alltid tillfälliga. Det betyder att filtreringen ska avslutas när hotet är över.

Det hör till varje teleföretags dagliga informationssäkerhetsarbete att bedöma behovet av och grunderna för tillfällig filtrering av trafiken för sina internetanslutningstjänster. På basis av sina iakttagelser om informationssäkerheten avgör teleföretaget i princip själv, huruvida filtreringen är nödvändig och hur länge den är nödvändig för att sörja för informationssäkerheten i nätet, i tjänsterna som tillhandahålls via nätet eller i slutanvändarnas terminalutrustning.

Transport- och kommunikationsverkets uppgift är däremot bland annat att:

- främja den elektroniska kommunikationens funktion, störningsfrihet och trygghet,
- samla in information om kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster och mervärdestjänster,
- informera om informationssäkerhetsärenden, och
- utreda kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster och mervärdestjänster.

Transport- och kommunikationsverket har också vissa bemyndiganden att meddela föreskrifter om informationssäkerhet.

När Transport- och kommunikationsverket sköter dessa uppgifter får det ibland veta om sådana informationssäkerhetshot som gör att det är allmänt motiverat för teleföretagen att filtrera trafik för internetanslutningstjänsterna. I ett sådant fall rekommenderar Transport- och kommunikationsverket i första hand att teleföretagen startar filtreringsåtgärder. Förpliktande bestämmelser åläggs endast vid behov och på basis av särskilt övervägande.

Verkets rekommendationer är inte tvingande. Det betyder att varje teleföretag bestämmer självt om de iakttar rekommendationen eller inte. Beaktansvärt är dock

att verket ger filtreringsrekommendationer endast efter noga övervägande. Ett teleföretag som beslutar att inte följa rekommendationen ska noga bedöma huruvida det i tillräcklig mån kan sörja för sina informationssäkerhetsskyldigheter utan att genomföra de filtreringsåtgärder som verket rekommenderat.

För att Transport- och kommunikationsverkets filtreringsrekommendationer, såväl gällande som tidigare, skulle finnas tillgängliga på ett ställe, har verket beslutat samla ihop sina filtreringsrekommendationer i denna för teleföretagen avsedda rekommendation. Filtreringsrekommendationerna har samlats in fr.o.m. nätneutralitetsreglernas ikraftträdande 30.4.2016. Verkets tidigare filtreringsrekommendationer som utfärdats före 30.4.2016 är inte längre i kraft.

I rekommendationen ges också ett förförande som verket följer när det ger nya filtreringsrekommendationer eller rekommenderar att filtrering ska avslutas.

1.2 Transport- och kommunikationsverkets förfarande

1.2.1 Bedömning av filtreringsbehov

Transport- och kommunikationsverket följer kontinuerligt upp det nationella informationssäkerhetsläget och bedömer om det finns behov för filtrering i teleföretagens internetanslutningstjänster.

Då Transport- och kommunikationsverket överväger att rekommendera filtrering eller avslutning av filtrering, tar verket hänsyn till i synnerhet följande frågor:

- Varför är filtrering nödvändig, dvs. vad är hotet eller kränkningen som man vill förebygga eller lindra genom filtreringen?
- Kan man skydda sig mot hotet på ett lindrigare sätt (t.ex. med användarnas egna åtgärder) än genom filtrering av trafik? Skulle den andra åtgärden vara tillräckligt effektiv? På vilka villkor?
- Vad kan det sannolikt eller i värsta fall hända utan filtrering? I vilken omfattning skulle konsekvenserna av att inte filtrera gälla teleföretag (det egentliga kommunikationsnätet eller den egentliga kommunikationstjänsten) och i vilken omfattning skulle de gälla slutanvändare?
- Hur inverkar filtreringen på slutanvändarnas tjänster, m.a.o. förhindrar filtreringen en allmänt använd tjänst och på vilket sätt, eller gäller de eventuella verkningarna en mycket liten användargrupp?
- Finns det en tidsram för filtrering, dvs. hur länge skulle filtreringen pågå?

När teleföretaget överväger om det behöver filtrera trafiken av informationssäkerhetsskäl, är det bra om företaget bedömer samma frågor i sin egen verksamhet.

1.2.2 Att ge och slopa en rekommendation om en viss kommunikationsport

När Transport- och kommunikationsverket ger en ny filtreringsrekommendation eller slutar rekommendera filtrering av trafik till en viss port, skickar verket ett meddelande om det till teleföretagen på följande sätt:

- Att ge en rekommendation: e-post till sändlistan FI-NSP med rubriken "*Rekommendation om filtrering av trafik för internetanslutningstjänster*"
- Att slopa en rekommendation: e-post till sändlistan FI-NSP med rubriken "*Rekommendation om att avsluta filtrering av trafik för internetanslutningstjänster*"

I meddelandet beskrivs orsaken till att ge eller slopa rekommendationen samt de tekniska detaljerna för genomförande (samma uppgifter som i kapitel 2).

Denna rekommendation uppdateras i enlighet med den rekommendation som ges per e-post så snart som möjligt efter meddelandet – i praktiken senast inom ett par vardagar. Den uppdaterade rekommendationen publiceras i verkets publikationsserie (på webbsidor). Detta tvåfasiga rekommendationsförfarande beror på praktiska orsaker: effektivt skydd mot informationssäkerhetshot och -kränkningar kräver ofta snabbhet och därför vill verket informera teleföretagen om de filtreringsbehov det beaktat så snart som möjligt. Genom ett rekommendationsförfarande i två faser ser verket till att en filtreringsrekommendation även kan ges utanför normal tjänstetid.

1.2.3 Åläggande av filtreringsskyldigheter

I första hand är det alltid en rekommendation av Transport- och kommunikationsverket att teleföretagen filtrerar trafik till vissa portar. Varje teleföretag bestämmer dock självt om de följer rekommendationen.

Om rekommendationen inte bidrar till tillräckligt skydd eller om en rekommenderad filtreringsåtgärd så småningom börjar bli permanent i stället att för vara tillfällig, överväger Transport- och kommunikationsverket att i enskilda fall ålägga teleföretag en filtreringsskyldighet.

Filtreringsskyldigheter åläggs genom teleföretagsspecifika beslut eller sannolikt genom att lägga till ett nytt filtreringskrav i föreskrift 67 om televerksamhetens informationssäkerhet, som är bindande för alla teleföretag. Det fanns ett filtreringskrav avseende en viss kommunikationsport i kraft när den första versionen av denna rekommendation gavs: teleföretag måste i princip förhindra trafik från konsumentabonnemang till port 25 om det sker via andra servrar än de som är avsedda för teleföretagets utgående SMTP-trafik.

1.2.4 Hörande av teleföretag

Denna rekommendation och det förfarande som beskrivs i kapitel 1.2.2 har varit på remiss hos teleföretagen när den första versionen av rekommendationen gavs (312/2017 S, 2.8.2017). Verket fick 6 utlåtanden. Det föreslogs inte några ändringar i de rekommendationer som gäller de egentliga portarna (tabell 1). Efter remissen gjordes följande ändringar och preciseringar i rekommendationen och rekommendationsförfarandet:

- Uppgift om sändlistan och rubriker som ska användas för att ge och slopa rekommendationer lades till i kapitel 1.2.2.
- Länkar till föreskrifter, beslut eller meddelanden som verket utfärdat lades till i tabell 2 för respektive informationssäkerhetsfenomen.
- Vissa skrivfel korrigerades.

Transport- och kommunikationsverket arrangerar inte någon separat remiss när det ger nya enstaka filtreringsåtgärder eller slopar dem. Hela rekommendationen skickas på remiss på nytt, om det görs ändringar i andra delar än i tabell 1 och 2.

När Transport- och kommunikationsverket överväger att ge en ny filtreringsrekommendation om trafik till en viss port eller slopa en existerande rekommendation, samarbetar verket naturligtvis med teleföretag som normalt och samlar in information och åsikter från teleföretag om informationssäkerhetsläget i enskilda fall och enligt behov för beslutsfattandet.

Om Transport- och kommunikationsverket överväger att ålägga filtreringsskyldigheter (antingen genom beslut eller genom föreskrift), hör verket teleföretag i enlighet med förvaltningslagen innan skyldigheten åläggs.

2 Transport- och kommunikationsverkets filtreringsrekommendationer

Transport- och kommunikationsverkets gällande rekommendationer om filtrering av trafik till en viss kommunikationsport finns i tabell 1. I tabell 1 visas rekommendationerna i portnummerordning.

När en filtreringsrekommendation slopas, flyttas den till tabell 2 som visar de rekommendationer som inte längre är i kraft. I tabell 2 visas de gamla rekommendationerna så att den senast slopade rekommendationen står överst. Tabell 2 innehåller alltså en s.k. historiklogg som omfattar alla tidigare rekommendationer.

För att få en helhetsbild av rekommendationerna i anslutning till filtrering omfattar tabellerna även information om skyldigheterna för filtrering, dvs. de obligatoriska filtreringarna. Vid utfärdande av den första versionen av denna rekommendation var ett obligatoriskt filtreringskrav för en viss kommunikationsport i kraft (föreskrift 67, 14 §).

Följande uppgifter visas i båda tabeller:

- Portnummer
  Här visas numret för den kommunikationsport som rekommendationen gäller.

- Protokoll
  Här beskrivs de kommunikationsprotokoll som rekommendationen gäller, dvs. endast TCP-protokollet, endast UDP-protokollet, eller båda.

- Riktning
  Här beskrivs den riktning som rekommendationen gäller, dvs. uppströms (Uplink, UL) eller nedströms (Downlink, DL), eller båda. Med uppströms (UL) avses trafik från kunder mot nätet och med nedströms (DL) trafik från nätet mot kunder.

- Tekniska preciseringar
  Här beskrivs eventuella tekniska preciseringar för filtrering. Utgångspunkten för rekommendationerna är att de gäller alla internetanslutningstjänster, dvs. såväl fasta som trådlösa nät samt abonnemang avsedda för både konsument- och företagsanvändning, om inget annat nämns i denna punkt i tabellen. Rekommendationerna gäller såväl IPv4- som IPv6-trafik, om inget annat nämns i denna punkt i tabellen. De tekniska preciseringarna kan även omfatta rekommendationer t.ex. om var i nätet filtreringen ska ske.

- Filtreringsåtgärd
  Här beskrivs hur trafiken mot en kommunikationsport ska filtreras: ska trafiken förhindras helt eller begränsas på något sätt.

- Orsak
  Här beskrivs i korthet orsaken till filtreringsåtgärden, dvs. varför filtreringen är nödvändig. Transport- och kommunikationsverket publicerar normalt särskilda meddelanden eller ger varningar om informationssäkerhetsfenomen vars skadliga verkningar filtreringsåtgärderna försöker lindra. I dessa publikationer beskriver verket fenomenets bakgrund och verkningar mera omfattande än i denna rekommendation.

I tabell 1 visas även filtreringsrekommendationens:

- Startdatum
  Här anges det datum när rekommendationen om en viss kommunikationsport gavs. I praktiken är datumet det datum då Transport- och kommunikationsverket har skickat teleföretagen ett e-postmeddelande om ny rekommendation.

I tabell 2 visas:

- Giltighetstid
  Här anges giltighetstiden för en slopad rekommendation, dvs. de datum då rekommendationen gavs och avlägsnades.

Tabell 1. Gällande filtreringsrekommendationer.

Port-nummer (mål-port)	Protokoll (TCP, UDP)	Riktning (UL, DL)[1]	Tekniska preciseringar	Filtreringsåtgärd (t.ex. förhindrande, begränsning)	Orsak	Startdatum
25	TCP	UL	Utförs på utgående trafik från konsumentabonnemang (se möjligheterna och förutsättningarna för undantag i föreskrift 67)	Förhindrande av TCP-trafik från kunden till port 25 via andra servrar än teleföretagets servrar för utgående SMTP-trafik	Skyldighet i föreskrift 67 (14 §, motivering MPS 67, https://www.kyberturvallisuus-keskus.fi/sv/saadokset-ohjeistukset-suositukset?query=67)	1.1.2015
53	UDP	DL	Utförs på trafik till konsumentabonnemang	Förhindrande av UDP-trafik till kundens port 53	Förhindrande av och skydd mot överbelastningsangrepp (DNS-reflektionsattack)	12.1.2018
123	UDP	DL	Utförs på trafik till konsumentabonnemang	Begränsning av trafik till kundens port 123 med metoder som inte förhindrar normal användning av NTP-klientprogram eller underhåll av servrar (t.ex. filtrering av NTP control mode-paket eller rate limiting-filtrering)	Förhindrande av och skydd mot överbelastningsangrepp (NTP-reflektionsangrepp)	12.1.2018
1900	UDP	DL	–	Förhindrande av UDP-trafik till kundens port 1900	Förhindrande av och skydd mot blockeringsattacker (SSDP-reflektionsangrepp)	13.2.2018

[1] Med upplänk (UL) avses trafik från kunden till nätet och med nerlänk (DL) trafik från nätet till kunden.

Tabell 2. Tidigare filtreringsrekommendationer som inte längre är i kraft.

Port-nummer (mål-port)	Proto-koll (TCP, UDP)	Rikt-ning (UL, DL)	Tekniska precise-ringar	Filtreringsåtgärd (t.ex. förhindrande, begränsning)	Orsak	Giltighetstid
53	UDP	DL	–	Förhindrande av trafik	Förhindrande av och skydd mot överbelast-ningsangrepp (DNS-reklektionsangrepp)	30.4.2016–12.1.2018
1900	UDP	UL och DL	–	Förhindrande av trafik	Förhindrande av och skydd mot överbelast-ningsangrepp (UPnP-protokollsårbarhet)	30.4.2016–12.1.2018
7547	TCP	UL och DL	–	Förhindrande av trafik	Förhindrande av och skydd mot överbelast-ningsangrepp (Mirai-botnätet)	28.11.2016–30.11.2020

3 Lagstiftning och föreskrifter

3.1 Nätneutralitet

Om nätneutralitet bestäms i EU:s förordning om den inre marknaden för elektronisk kommunikation, dvs. i Europaparlamentets och rådets förordning 2015/2120[2] som är direkt tillämplig i medlemsstaterna. I 110 § i lagen om tjänster inom elektronisk kommunikation[3] (917/2014, tidigare informationssamhällsbalken) finns en informativ hänvisning till förordningen.

I artikel 3 i förordningen behandlas skyddet för öppen internetanslutning, dvs. principen för nätneutralitet (net neutrality):

> "*1. Slutanvändare ska ha rätt att via sin internetanslutningstjänst ha tillgång till och distribuera information och innehåll, använda och tillhandahålla applikationer och tjänster och använda terminalutrustning efter eget val, oavsett var slutanvändaren eller leverantören befinner sig och oavsett informationens, innehållets, applikationens eller tjänstens lokalisering, ursprung eller destination.*
>
> *Denna punkt påverkar inte tillämpningen av unionsrätten och med unionsrätten förenlig nationell rätt rörande innehålls, applikationers eller tjänsters laglighet.*
>
> *2. Överenskommelser mellan leverantörer av internetanslutningstjänster och slutanvändare om kommersiella och tekniska villkor och de egenskaper för internetanslutningstjänster, såsom pris, datavolymer och datahastighet, och eventuella affärsmetoder som tillämpas av leverantörer av internetanslutningstjänster, får inte begränsa utövandet av slutanvändares rättigheter som anges i punkt 1.*
>
> *3. Leverantörer av internetanslutningstjänster ska behandla all trafik likvärdigt, utan diskriminering, begränsningar eller störanden, och oberoende av sändare och mottagare, det innehåll användarna tar del av eller distribuerar, de applikationer eller tjänster som används eller tillhandahålls eller den terminalutrustning som används.*
>
> *Det första stycket ska inte hindra leverantörer av internetanslutningstjänster från att genomföra rimliga trafikstyrningsåtgärder. För att anses vara rimliga ska sådana åtgärder vara öppna, icke-diskriminerande och proportionella och ska inte grundas på kommersiella överväganden utan på objektiva sett skilda krav på tjänstens tekniska kvalitet för specifika kategorier av trafik. Sådana åtgärder får inte övervaka det specifika innehållet och får inte bibehållas längre än vad som är nödvändigt.*
>
> *Leverantörer av internetanslutningstjänster får inte tillämpa trafikstyrningsåtgärder som går utöver de som anges i andra stycket och får i synnerhet inte blockera, sakta ned, ändra, begränsa, störa, försämra eller diskriminera specifikt innehåll, specifika applikationer eller tjänster eller specifika kategorier av dessa, utom när det är nödvändigt, och endast så länge det är nödvändigt, för att*

[2] Europaparlamentets och rådets förordning (EU) 2015/2120 av den 25 november 2015 om åtgärder rörande en öppen internetanslutning och slutkundsavgifter för reglerad kommunikation inom EU och om ändring av direktiv 2002/22/EG och förordning (EU) nr 531/2012: http://data.europa.eu/eli/reg/2015/2120/oj.

[3] https://www.finlex.fi/sv/laki/smur/2014/20140917

a) följa unionens lagstiftningsakter eller med unionsrätten förenlig nationell lagstiftning som leverantören av internetanslutningstjänster omfattas av, eller åtgärder som är förenliga med unionsrätten som ger verkan åt sådana unionslagstiftningsakter eller nationell lagstiftning, inklusive rättsliga avgöranden eller beslut från myndigheter med relevanta befogenheter,

b) bevara robustheten och säkerheten i nätet, tjänster som tillhandahålls via det nätet och slutanvändarnas terminalutrustning,

c) förhindra en nära förestående överbelastning av nätet eller lindra effekterna av exceptionell eller tillfällig överbelastning av nätet, under förutsättning att likvärdiga kategorier av trafik behandlas likvärdigt.

--."

3.2 Informationssäkerhetsskyldigheter och -rättigheter

I 243 § i lagen om tjänster inom elektronisk kommunikation bestäms om kvalitetskrav på kommunikationsnät och kommunikationstjänster:

"Allmänna kommunikationsnät och kommunikationstjänster samt kommunikationsnät och kommunikationstjänster som ansluts till dem ska planeras, byggas och underhållas så att

1) den elektroniska kommunikationens tekniska standard är god och informationssäker,

2) de tål sådana normala klimatrelaterade, mekaniska, elektromagnetiska och andra yttre störningar samt hot mot informationssäkerheten som kan förväntas,

--

4) mot dem riktade betydande kränkningar av och hot mot informationssäkerheten kan upptäckas liksom också sådana fel och störningar som avsevärt stör deras funktion,

--

7) inte någons dataskydd, informationssäkerhet eller andra rättigheter äventyras,

--

9) de inte orsakar oskäliga elektromagnetiska eller andra störningar eller hot mot informationssäkerheten,

--.

De åtgärder för att sörja för informationssäkerheten enligt 1 mom. 1, 2, 4, 7 och 9 punkten avser åtgärder för att trygga säkerheten i fråga om verksamheten, datatrafiken, utrustningen, programmen och datamaterialet. Åtgärderna ska anpassas till hur allvarliga hot som föreligger, till kostnaderna för åtgärderna och till de tekniska möjligheter att avvärja hoten som står till buds.

--."

I 247 § i lagen om tjänster inom elektronisk kommunikation bestäms om skyldigheten att sörja för informationssäkerheten vid kommunikationsförmedling (bl.a. teleföretag) och tillhandahållande av mervärdestjänster:

"Den som förmedlar kommunikation ska vid förmedlingen sörja för informationssäkerheten när det gäller tjänsterna, meddelandena, förmedlingsuppgifterna och lokaliseringsuppgifterna. En sammanslutningsabonnent som förmedlar kommunikation ska dock endast sörja för informationssäkerheten i fråga om behandlingen av sina användares meddelanden, förmedlingsuppgifter och lokaliseringsuppgifter.

--

De åtgärder som vidtas för informationssäkerheten ska anpassas till hotets allvarlighet, till kostnaderna för åtgärderna samt till de tekniska möjligheter att avvärja hotet som står till buds.

--."

I 272 § i lagen om tjänster inom elektronisk kommunikation bestäms om åtgärder för informationssäkerheten:

"Teleföretag, sammanslutningsabonnenter och leverantörer av mervärdestjänster samt aktörer som handlar för dessas räkning har rätt att vidta nödvändiga åtgärder enligt 2 mom. för att sörja för informationssäkerheten i syfte att

1) upptäcka, förhindra och utreda störningar som kan inverka menligt på informationssäkerheten i kommunikationsnäten eller tjänster som anslutits till dem samt i informationssystemen och göra störningarna föremål för förundersökning,

2) trygga kommunikationsmöjligheterna för den som sänder eller tar emot meddelanden, eller

3) förhindra i 37 kap. 11 § i strafflagen avsedd förberedelse till sådana betalningsmedelsbedrägerier som planeras bli genomförda i omfattande utsträckning via kommunikationstjänsterna.

Åtgärder som avses i 1 mom. kan omfatta

1) automatisk analys av innehållet i meddelanden,

2) automatiskt förhindrande eller automatisk begränsning av förmedling och mottagande av meddelanden,

3) automatiskt avlägsnande av sådana skadliga datorprogram ur meddelandena som kan äventyra informationssäkerheten,

4) andra åtgärder av teknisk natur som är jämförbara med dem som avses i 1–3 punkten.

Om det utifrån typen av meddelande, meddelandets form eller någon annan motsvarande omständighet är uppenbart att ett meddelande innehåller ett skadligt datorprogram eller ett skadligt kommando och uppnåendet av målen enligt 1 mom. inte kan säkerställas genom åtgärder som avses i 2 mom. 1 punkten, får innehållet i ett enskilt meddelande behandlas manuellt. Avsändaren och mottagaren av meddelandet ska underrättas om den manuella behandlingen av innehållet, om det inte är så att underrättelsen sannolikt äventyrar uppnåendet av målen enligt 1 mom.

Åtgärder enligt denna paragraf ska utföras omsorgsfullt och de ska stå i proportion till den störning som avvärjs. Åtgärderna ska utföras utan att

yttrandefriheten, skyddet av konfidentiella meddelanden eller integritetsskyddet begränsas mer än vad som är nödvändigt med tanke på säkerställandet av möjligheterna att uppnå målen enligt 1 mom. Åtgärderna ska avslutas, om det inte längre finns förutsättningar enligt denna paragraf att vidta dem."

Med hänsyn till skyldigheterna ovan får Transport- och kommunikationsverket enligt lagen om tjänster inom elektronisk kommunikation meddela vissa föreskrifter som preciserar lagen.

Transport- och kommunikationsverkets företrädare Kommunikationsverket har meddelat föreskrift 67 om televerksamhetens informationssäkerhet[4]. Föreskriften innehåller närmare föreskrifter om:

- åtgärder som ska vidtas i fråga om informationssäkerheten i alla kommunikationsnät och -tjänster,
- särskilda krav på informationssäkerheten i gränssnitt,
- särskilda krav för internetaccesstjänster,
- särskilda krav för e-posttjänster, och
- information till kunderna om informationssäkerhet.

[4] https://www.kyberturvallisuuskeskus.fi/sv/saadokset-ohjeistukset-suositukset?query=67