TRAFICOM/248815/03.04.05.00/2022
28.11.2023

Motiveringspromemoria till den meddelade föreskriften om informationssäkerhet inom televerksamheten

Innehåll

I. Föreskriftens bakgrund och rättsgrund

Föreskriften har samband med 29 kap. i lagen om tjänster inom elektronisk kommunikation (917/2014), som innehåller bestämmelser om kvalitetskrav på kommunikationsnät och kommunikationstjänster och kommunikationsförmedlarnas, såsom teleföretagens, skyldighet att svara för informationssäkerheten när det gäller tjänsterna, meddelandena, förmedlingsuppgifterna och lokaliseringsuppgifterna, samt med 33 kap., som i sin tur innehåller bestämmelser om hantering av informationssäkerhet och störningar samt anmälan om störningar.

Kvalitetskrav på kommunikationsnät och kommunikationstjänster

Föreskriften har samband med 243 § 1 mom. 1, 2, 7, 9, 10, 11 och 13 punkten i lagen om tjänster inom elektronisk kommunikation, enligt vilka allmänna kommunikationsnät och -tjänster samt de kommunikationsnät och -tjänster 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,

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

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

10) de är interoperabla och att kommunikationsnäten vid behov kan anslutas till andra kommunikationsnät,

11) ändringar som görs i dem inte orsakar oförutsedda störningar i andra kommunikationsnät och kommunikationstjänster,

13) den aktör som ansvarar för dem också i övrigt kan uppfylla sina skyldigheter eller de skyldigheter som följer av denna lag.

Enligt 243 § 2 mom. i lagen om tjänster inom elektronisk kommunikation ska de kvalitetskrav som avses i 1, 2, 10 och 11 punkten anpassas till antalet användare av kommunikationsnäten och -tjänsterna, till det geografiska område som de betjänar samt till deras betydelse för användarna.

De åtgärder för att sörja för informationssäkerheten enligt 1, 2, 7 och 9 punkten avser enligt 243 § 3 mom. i lagen om tjänster inom elektronisk kommunikation 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.

Enligt lagens 243 § 4 mom. gäller de kvalitetskrav som avses i 243 § 1 mom. också betydande tillhörande faciliteter och tillhörande tjänster i samband med kommunikationsnät och kommunikationstjänster[1].

[1] Enligt 3 § 1 mom. 8 punkten i lagen om tjänster inom elektronisk kommunikation avses med *tillhörande tjänster* system för villkorad tillgång, elektroniska programguider och nummeromvandling, tjänster för identifiering, lokalisering och lägesinformation samt andra sådana motsvarande tjänster i samband med kommunikationsnät eller kommunikationstjänster som gör det möjligt att tillhandahålla kommunikationsnät eller kommunikationstjänster eller som stödjer tillhandahållande av tjänster via dem. Enligt 9 punkten i samma

I denna föreskrift preciseras de ovan nämnda tekniska kraven enligt 243 § med stöd av 244 § 2, 3, 5, 8, 12, 13, 14 och 16 punkterna i lagen, enligt vilka Transport- och kommunikationsverkets föreskrifter kan gälla:

2) elektroniskt och fysiskt skydd av kommunikationsnät och tillhörande utrustningsutrymmen,

3) prestanda, informationssäkerhet och störningsfrihet, underhåll och uppföljning av dessa samt nätverksadministration,

5) kommunikationsnätets konstruktion samt tekniska egenskaper hos anslutningspunkter i kommunikationsnätet,

8) samtrafik, kompatibilitet, signalering och synkronisering,

12) teknisk dokumentation och statistik samt utformning av tillhörande dokument och lagring av uppgifter,

13) standarder som ska iakttas,

14) tillhörande faciliteter och tillhörande tjänster till den del som de är relevanta för de krav enligt 243 § som ställs på kommunikationsnät och kommunikationstjänster,

16) andra jämförbara tekniska krav på kommunikationsnät och kommunikationstjänster.

I lagens 247 § finns bestämmelser om kommunikationsförmedlarens, liksom även teleföretagets, skyldighet att sörja för informationssäkerheten. Enligt paragrafens 1 mom. ska den som förmedlar kommunikation vid förmedlingen sörja för informationssäkerheten när det gäller tjänsterna, meddelandena, förmedlingsuppgifterna och lokaliseringsuppgifterna. Enligt 3 mom. ska de åtgärder som vidtas för informationssäkerheten anpassas till hotets allvarlighet, till kostnaderna för åtgärderna samt till de tekniska möjligheter att avvärja hotet som står till buds.

Med stöd av 247 § 4 mom. i lagen får Transport- och kommunikationsverket meddela närmare föreskrifter om bl.a. informationssäkerheten enligt 1 mom.

Med förmedlingsuppgifter avses enligt 3 § 40 punkten i lagen om tjänster inom elektronisk kommunikation (i lagen 456/2016) information som kan kopplas till en juridisk eller fysisk person och som behandlas för att överföra meddelanden, samt uppgifter om en radiostations identifieringssignal och radiosändarens användare samt om radiosändningens starttid, varaktighet och utsändningsplats. Enligt 3 § 22 punkten i lagen om tjänster inom elektronisk kommunikation avses med elektroniskt meddelande information som förmedlas eller distribueras elektroniskt.

Hantering av informationssäkerhet och störningar

I 272 § i lagen om tjänster inom elektronisk kommunikation föreskrivs om teleföretags och vissa andra aktörers åtgärder för informationssäkerheten. Enligt paragrafens 1 mom. har dessa aktörer rätt att vidta nödvändiga åtgärder enligt 2 mom. för att sörja för informationssäkerheten i syfte att:

bestämmelse avses med *tillhörande faciliteter* i sin tur tillhörande tjänster samt byggnader, tillträde till byggnader, kablar, kabelkanaler, master och annan sådan motsvarande fysisk infrastruktur och faciliteter och komponenter i samband med kommunikationsnät eller kommunikationstjänster som gör det möjligt att tillhandahålla kommunikationsnät eller kommunikationstjänster eller som stödjer tillhandahållande av tjänster via dem.

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 till 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.

Enligt paragrafens 3 mom. får innehållet i ett enskilt meddelande behandlas manuellt, 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. 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.

Enligt 4 mom. i den aktuella paragrafen ska åtgärder enligt paragrafen 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.

I föreskriften preciseras med stöd av 272 § 5 mom. i lagen om tjänster inom elektronisk kommunikation hur de åtgärder som avses ovan ska genomföras tekniskt.

Föreskriften och i synnerhet skyldigheterna beträffande bortkoppling av internetaccesstjänster enligt den hänger även samman med 273 § i lagen om tjänster inom elektronisk kommunikation, där det föreskrivs om skyldigheten att avhjälpa störningar. I paragrafens 1 mom. står det föreskrivet att, om ett kommunikationsnät, en kommunikationstjänst eller en utrustning orsakar betydande olägenheter eller störningar för ett kommunikationsnät, en kommunikationstjänst, någon annan tjänst som anslutits till kommunikationsnätet, utrustning, eller för kommunikationsnätets användare eller någon annan person, ska teleföretaget eller en annan innehavare av kommunikationsnätet eller utrustningen omedelbart vidta åtgärder för att avhjälpa situationen och vid behov koppla bort kommunikationsnätet, kommunikationstjänsten eller utrustningen från det allmänna kommunikationsnätet.

Enligt 273 § 2 mom. i lagen ska ovan avsedda åtgärder 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.

Transport- och kommunikationsverket kan i sådana fall som avses i 273 § 1 mom. i lagen om tjänster inom elektronisk kommunikation besluta om avhjälpande åtgärder samt om bortkoppling av ett nät, en tjänst eller en utrustning.

II. Transport- och kommunikationsverkets övriga relaterade föreskrifter och rekommendationer

I detta kapitel beskrivs Transport- och kommunikationsverkets övriga föreskrifter, rekommendationer och anvisningar som har samband med föreskriftens ämnesområde.[2]

I föreskriften *om störningar i televerksamheten* hanteras olika störningar i televerksamheten. Föreskriften gäller både situationer där teleföretagets tjänster utsätts för en betydande kränkning av informationssäkerheten eller hot om densamma (*informationssäkerhetsstörning*) och händelser som förhindrar eller på ett väsentligt sätt stör kommunikationstjänstens funktion (*funktionsstörning*). Föreskriften ålägger teleföretag skyldigheter som gäller såväl observation och hantering av störningar i informationssäkerheten och i funktionen som att anmäla och föra statistik över dem.

I föreskriften om *kommunikationsnätets kritiska delar* föreskrivs om identifikation av kommunikationsnätets kritiska delar och dokumentering samt ges närmare föreskrifter än i lagen om definitionen av de kritiska delarna i kommunikationsnät.

Föreskriften om *säkerställande av kommunikationsnät och kommunikationstjänster samt om synkronisering av kommunikationsnät* ställer minimikrav på teleföretag om bland annat säkerställandet av effektmatning till utrustning som används för att tillhandahålla kommunikationsnätverk eller kommunikationstjänster, säkerställandet av utrustning och anslutningar samt fysiskt skydd av utrustning.

Föreskriften om *elektroniskt skydd av kommunikationsnät* innehåller skyldigheter som gäller skyddandet av allmänna kommunikationsnät samt till dessa anslutna utrustningar och kommunikationsnät mot överspänningar och överströmmar som är av atmosfäriskt ursprung eller orsakas av elanläggningar.

Föreskriften *om kommunikationsnätens och -tjänsternas kvalitet samt om samhällsomfattande tjänster* gäller mätning och kontroll av kommunikationsnäten och -tjänsternas driftssäkerhet, prestanda, tillförlitlighet och kvalitet. Föreskriften omfattar allmänna skyldigheter som tillämpas på alla kommunikationsnät och -tjänster samt speciella krav som gäller telefonitjänster, internetförbindelsetjänster och televisionstjänster.

Föreskriften *om tekniskt genomförande och säkerställande av nödtrafik* innehåller krav med vilka det säkerställs att nödsamtal och nödtextmeddelanden samt därtill relaterad, för nödtjänsten väsentlig information överförs från de allmänna kommunikationsnäten till nödcentralerna. Föreskriftens krav säkerställer också att nödsamtalen har bättre möjligheter att lyckas än normala samtal vid olika slags belastningar och störningar i kommunikationsnätet.

[2] Föreskrifter, anvisningar och offentliga rekommendationer finns på sidan https://www.traficom.fi/sv/foreskrifter?group=cybersakerhet.

Rekommendationen till teleföretag om beredskap ger teleföretag råd om hur beredskapskraven i lagen kan uppfyllas. Rekommendationen, som är delvis sekretessbelagd, är inte en allmän och allmäntäckande anvisning om förberedelse-, kontinuitets eller beredskapsplanering och genomförandet av dessa, utan i den har man lyft fram frågor som Transport- och kommunikationsverket rekommenderar att teleföretagen tar i beaktande som en del av deras beredskapsskyldighet och befintlig beredskapspraxis.

Rekommendationen om *informationssäkerhetsbaserad filtrering av trafik till vissa kommunikationsportar i teleföretagens nät* gäller filtrering av trafiken i internetaccesstjänster.

Rekommendationen om information om informationssäkerheten i tjänster som genomförts i utlandet gäller hurdan information användare ska ges om kommunikationstjänster med en internationell koppling och på vilket sätt. En del av teleföretagen genomför sina kommunikationstjänster helt eller delvis i länder utanför Finland eller med hjälp av tjänster som tillhandahålls av utländska företag. Därför kan genomförandet av tjänsterna omfattas av regler som skiljer sig från Finlands lagstiftning och som användarna av tjänsterna ska få information om. Utöver att teleföretaget sörjer för informationssäkerheten för sin tjänst även i dessa situationer kan användaren själv med hjälp av sådan information bedöma vilka eventuella hot som är förknippade med hans eller hennes kommunikation och förmedlingsuppgifter.

Rekommendationen *Common Nordic Recommendations on SS7 Security Issues* innehåller åtgärder för att förbättra säkerheten för SS7-signalering. Rekommendationen är sekretessbelagd.

Anvisningen om dokumentation av uppgifter som gäller behandling av förmedlingsuppgifter innehåller anvisningar om tillämpningen av 145 § i lagen om tjänster inom elektronisk kommunikation. I paragrafen föreskrivs om kommunikationsförmedlares skyldighet att dokumentera detaljerade loggdata om behandlingen av förmedlingsuppgifter i informationssystem som innehåller förmedlingsuppgifter med central betydelse för konfidentialiteten och integritetsskyddet, om det är tekniskt möjligt utan oskäliga kostnader.

III. Föreskriftens syfte

Föreskriftens syfte är att:

1. främja informationssäkerheten i allmänna kommunikationsnät och -tjänster,
2. trygga den elektroniska kommunikationens konfidentialitet och värna om integritetsskyddet, och
3. säkerställa att informationssäkerheten genomförs i teleföretagen på ett övergripande, systematiskt och effektivt sätt.

Kraven i föreskriften syftar till att uppnå dessa mål, och tillämpningen av föreskriften styrs av målen. Ovanstående mål bör utgöra utgångspunkten i alla frågor rörande genomförandet av informationssäkerheten i den allmänna televerksamheten.

Med informationssäkerhet avses enligt 3 § 1 mom. 28 punkten i lagen om tjänster inom elektronisk kommunikation ”administrativa och tekniska åtgärder genom vilka det säkerställs att information är tillgänglig endast för dem som har rätt att använda den, att informationen inte kan ändras av andra än dem som har rätt till detta samt att informationen och informationssystemen kan utnyttjas av dem som har rätt att använda informationen och systemen”. Informationssäkerhet innebär med andra ord åtgärder för att säkerställa kommunikationens konfidentialitet, integritet och användbarhet. Syftet med föreskriften är att främja att dessa mål ska uppnås.

I föreskriften definieras minimikraven för att genomföra informationssäkerheten. Avsikten med föreskriften är att beaktandet av informationssäkerhet i teleföretag blir en del av den dagliga verksamheten. Med andra ord försöker man genom föreskriften garantera att möjliga informationssäkerhetsfaktorer beaktas i rutinen och genom effektiva processer som en del av tillhandahållandet av kommunikationsnätverk och dess tjänster.

IV. Andra alternativ för verkställandet

I detta kapitel beskrivs andra alternativa genomförandesätt som övervägts i samband med beredningen av föreskriften.

Föreskriftens tillämpningsområde

Den tidigare föreskriftens tillämpningsområde begränsades till allmän televerksamhet, med undantag av skyldigheten att förhindra störningar (9.1 §) som dessutom tillämpades på myndighetsnät som sammankopplats med ett allmänt kommunikationsnät. Under beredningen av föreskriften bedömde Transport- och kommunikationsverket behovet av att utvidga tillämpningsområdet till förutom myndighetsnät, även till exempelvis sådana lokala mobilnät som inte är allmänna kommunikationsnät eller till s.k. kritiska separata nät som har definierats i föreskriften om kommunikationsnätets kritiska delar. Under beredningen i arbetsgruppen framkom dock inget tydligt behov av detta. I 273 § i lagen om tjänster inom elektronisk kommunikation föreskrivs i varje fall om den allmänna skyldigheten att avhjälpa störningar. Vid avtal om samtrafik är det dessutom möjligt att beakta kraven som gäller informationssäkerheten. Därför bedömde man att det inte är nödvändigt att utvidga tillämpningsområdet för motsvarande punkt (15.1) i den nya föreskriften till privata nät.

I utvidgningen av tillämpningsområdet beaktades dock modellen för genomförande av Virve 2.0, där nättjänsten i stället för det traditionella myndighetsnätet produceras av ett teleföretag (en nättjänst som betjänar myndighetskommunikation) och tillhandahållare av kommunikationstjänster med anknytning till myndighetskommunikation. Tillämpningen av den nya föreskriften utvidgades även till att omfatta de sistnämnda för att föreskriftens tillämpningsområde i praktiken inte skulle begränsas jämfört med tidigare.

Precisering av skyldigheter som gäller beaktande av informationssäkerheten

I den tidigare föreskriften definierades de delområden av informationssäkerheten som ska beaktas endast på ett allmänt plan. Även om definitionssättet var flexibelt förblev dess vägledande effekt enligt Transport- och kommunikationsverkets erfarenhet på motsvarande sätt mycket allmän. Därför bedömde Transport- och kommunikationsverket i samband med beredningen av föreskriften alternativen att kvarhålla det tidigare definitionssättet, att komplettera det med mer detaljerade kriterier eller att helt och hållet ändra definitionssättet så att man i föreskriften mycket direkt skulle stödja sig på de delområden av informationssäkerheten som Europeiska unionens cybersäkerhetsbyrå ENISA fastställt.[3]

I en enkät[4] som genomfördes sommaren 2022 ansåg de som gav utlåtanden i frågan att skyldigheten i den tidigare föreskrift inte var för allmän. I utlåtandena lyftes fram

[3] ENISA Guideline on security measures under the EECC, 4th Edition, July 2021 (nedan ENISAs riktlinjer eller ENISA GL).
[4] Uppdatering av föreskriften om televerksamhetens informationssäkerhet (67 A/2015 M): Enkät om erfarenheter och utvecklingsidéer, dnr Traficom/16241/09.09/2022.

att skyldigheterna bör vara tillräckligt allmänna så att teleföretagen själva kan välja informationssäkerhetslösningar.

Transport- och kommunikationsverket anser att en mer exakt definition än tidigare ändå är nödvändig för att främja föreskriftens mål och förbättra den styrande effekten av föreskriften. Det tidigare relativt allmänna sättet att definiera skyldigheterna har inte främjat till exempel tillsynen och övervakningen, eftersom man i föreskriften inte ställde mer detaljerade skyldigheter för de olika delområdena, vars genomförande man i kontrollerna kunde ha övervakat individuellt. Ämbetsverket övervägde även mellan alternativen att komplettera det tidigare definitionssättet och att anta ett angreppssätt i enlighet med ENISA. Transport- och kommunikationsverket anser att det som stödjer valet av ENISAs angreppssätt är att man i genomförandet av skyldigheterna i sådana fall kan stödja sig på ENISAs fastställda och rekommenderade informationssäkerhetskontroller. I sådana fall är dokumenteringen av efterlevnaden av kraven i teleföretag och övervakningen av dem ur myndighetens synvinkel båda enklare jämfört med om teleföretagen skulle vara tvungna att upprätta dokumentation om samma eller liknande skyldigheter som är indelad på ett annat sätt jämfört med föreskriften, vilket skulle orsaka extra arbete. Genom att välja ENISAs angreppssätt och använda de kontroller som ENISA rekommenderar undviker man med tanke på multinationella teleföretag uppkomsten av avvikande nationella krav och främjar även möjligheterna att använda samma dokumentation i olika länder.

Iakttagande av vissa standarder som gäller mobilnät

I den tidigare versionen av föreskriften ingick inga skyldigheter beträffande iakttagandet av standarder. Det finns inga säkerhetsstandarder som gäller för all televerksamhet i allmänhet, men det finns standarder för olika tekniker och funktioner som man kan använda för att säkerställa att allmänt vedertagen praxis iakttas.

5G-mobilnäten och de nya tjänster som de möjliggör kommer att ha en central roll för informationssamhället och ekonomin. Vid sidan av 5G-nätet har LTE-tekniken ännu länge en väsentlig roll som basteknologi för mobilnätet. Därför är det uttryckligen viktigt att ta hand om informationssäkerheten för dessa nät samtidigt som 5G-teknikens mer komplexa teknikmiljö ställer högre krav på riskhanteringen.[5]

Vikten av att säkerställa säkerheten i mobilnäten som en del av samhällets kritiska infrastruktur blir allt större. Standardiseringsorganisationerna (3GPP) har för sin del svarat på oron över säkerheten genom att utarbeta säkerhetsstandarder, med hjälp av vilka tillverkarna och mobilnätets teleföretag på ett transparent sätt kan bevisa och bestyrka genomförandet av nödvändiga säkerhetsåtgärder i sina system samt sina kommunikationsnät och -tjänster. Säkerhetsstandarderna är samlingsstandarder i vilka man har sammanställt viktiga åtgärder i fråga om säkerheten i 4G- och 5G-enheter.

Transport- och kommunikationsverket anser att det är motiverat att granska hur standarder som fokuserar i synnerhet på nyare mobilnätsgenerationers säkerhet kan utnyttjas i föreskriften och i teleföretagens egen verksamhet som en del av genomförandet av den övergripande säkerheten i mobilnäten. I föreskriftsarbetsgruppen förhöll sig en del av medlemmarna negativt till de föreslagna hänvisningarna till de bindande punkterna i standarderna, eftersom ett detaljerat genomförande av standarderna ansågs

[5] Se Sammanfattning av rapporten om cybersäkerheten i 5G (på finska, Selvitys 5G:n kyberturvallisuudesta, Yhteenveto), Traficoms publikationer 14.05.2019, https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Selvitys%205Gn%20kyberturvallisuudesta%20yhteenveto.pdf samt Cybersecurity of 5G networks EU Toolbox of risk mitigating measures, NIS Cooperation Group, CG Publication 01/2020 (nedan 5G Toolbox), s. 3–4.

begränsa teleföretagens verksamhetsmöjligheter vid valet av säkerhetslösningar och möjligtvis även vid valet av tillverkare. Dessutom ansågs det vara ett problem att en detaljerad lista snabbt skulle bli föråldrad när standarderna uppdateras, varvid en lista som gjorts upp i samband med uppdatering av föreskriften inte längre fullt ut skulle motsvara säkerhetsbehoven.

Transport- och kommunikationsverket har bedömt följande alternativ för genomförandet för att sörja för säkerhetskraven för mobilnät:

1. Inga hänvisningar på föreskriftsnivå till enskilda standarder eller säkerhetsåtgärderna i dem. Alternativet kan kompletteras med en hänvisning av rekommendationen till säkerhetsstandarderna i motiveringspromemorian.
2. Genom föreskriften åläggs förpliktelse att iaktta vissa punkter om mobilnätstandarder per punkt i föreskriften.
3. Genom föreskriften åläggs förpliktelse att allmänt följa de uppräknade standarderna.

Transport- och kommunikationsverket anser att utnyttjande av 3GPP:s standarder är en fungerande metod för att säkerställa att de komponenter som används vid förverkligandet av näten och tjänsterna uppfyller cybersäkerhetkraven på basnivå. Genom att hänvisa till standarderna kan man se till att färdigt definierade säkerhetsåtgärder i så stor utsträckning som möjligt blir genomförda och införda på ett lämpligt sätt. Ett sådant mål skulle inte uppfyllas enbart genom rekommendationen om att följa standarderna, och därför valdes inte alternativ 1. En lösning som kräver att standarderna följs har också nåtts åtminstone i Österrike och Tyskland, där kraven på att 3GPP-standarderna följs har fastställts som en del av förbättringen av säkerheten i mobilnäten.[6]

Alternativ 2 valdes inte eftersom standarderna är teknikspecifika och hänvisningen till 3GPP-standarderna för mobilnät inte är en ändamålsenlig lösning för allmänt förpliktande punkter i föreskriften. Även i övrigt skulle förpliktande hänvisningar till enskilda punkter i standarderna i onödan öka föreskriftens komplexitet och behovet av att uppdatera den.

Alternativ 3 valdes och man beslöt att genomföra det med standardbilagan till föreskriften, eftersom det var det mest genomförbara alternativet. Syftet med skyldigheten är inte att förutsätta att teleföretagen genom egna åtgärder verifierar att de komponenter som leverantörerna levererar uppfyller tillämpliga krav, utan att lämpliga förfaranden införs för att på de sätt som teleföretaget fastställt se till att de säkerhetsfunktioner som beskrivs i standarderna beaktas och vid behov genomförs i teleföretagets verksamhet under systemens hela livscykel. Avsikten är inte att man genom skyldigheten ska påverka leverantörernas produktutvecklingscykler, utan säkerställa att de säkerhetsfunktioner som teleföretaget infört för åtgärdernas versioner i standarderna beaktas fullt ut eller att underlåtenheten att följa dem motiveras och riskerna hanteras på andra sätt.

BGP-routing

I den tidigare versionen av föreskriften hade man inte på ett uttömmande sätt tagit ställning till säkerhetsfaktorerna beträffande BGP. BGP är ett centralt routingprotokoll för internet som, när det utsätts för oavsiktliga eller avsiktliga störningar, kan orsaka

[6] BSI Technical Guideline TR-03163: Security in Telecommunications Infrastructure samt Verordnung der Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH) über Verpflichtungen von Betreibern elektronischer Kommunikationsnetze und Anbietern elektronischer Kommunikationsdienste im Zusammenhang mit Mindestsicherheitsmaßnahmen unter Berücksichtigung von 5G-Netzen sowie mit Informationspflichten bei Sicherheitsvorfällen – Telekom-Netzsicherheitsverordnung 2020 (TK-NSiV 2020) § 6(2) och bilaga 1 (https://www.ris.bka.gv.at/eli/bgbl/II/2020/301/20200703).

allvarliga konsekvenser för informationssäkerheten. Det finns inga inbyggda säkerhetsfunktioner i BGP-routingprotokollet, vilket har lett till en situation där säkerheten i BGP närmast ombesörjs genom säkerhetsegenskaper som byggts på protokollet i efterhand. De säkerhetsfunktioner som valts till föreskriften grundar sig på ENISAs informationssäkerhetsrekommendationer för BGP[7].

Transport- och kommunikationsverket utredde sommaren 2022 läget för införandet av BGP-säkerhetsfaktorer i teleföretagen. Enkäten gällde ENISAs informationssäkerhetsrekommendationer[7] i anknytning till BGP:s säkerhet.

En del av faktorerna som förbättrar informationssäkerheten i BGP har angetts som exempel i denna motiveringspromemoria. Det har inte ålagts någon skyldighet att använda dem, eftersom Transport- och kommunikationsverket inte har ansett att de är nödvändiga vid tidpunkten för utfärdandet av denna föreskrift. Nödvändigheten har bedömts utifrån säkerhetsegenskapernas effekter.

Med tanke på både BGP:s centrala roll i internetrouting och den interna otryggheten i protokollet i fråga har Transport- och kommunikationsverket ansett det nödvändigt att ålägga teleföretagen skyldigheter som upprätthåller och förbättrar säkerheten i BGP.

Särskilda krav för gränssnitt

I den tidigare föreskriften gällde kapitel 3 förhindrande av och skydd mot störningar i samtrafik- och kundgränssnitt, stängning av obehövliga tjänster och protokoll samt hindrande av IP-trafik i samtrafik- och kundgränssnitt. Kommunikationsnätens utveckling, nya användningsfall och tjänstebaserade arkitekturlösningar (SBI) har ökat nya gränssnitt i teleföretagens kommunikationsnät. Därtill används de äldre nätgenerationernas signaleringsprotokoll fortfarande på bred front vid sidan om de nya signaleringsprotokollen.

I enkäten som genomfördes sommaren 2022 före utarbetandet av föreskriften hade de som gav utlåtanden en varierande inställning till förutsättningen att skydda signaleringsgränssnitt. I en del av svaren såg man inget behov av närmare reglering. En del ansåg att idén var god, men att kravet bör hållas på en allmän nivå. I ett av utlåtandena lyftes fram att det bör förutsättas att teleföretag genomför alla de åtgärder genom vilka man säkerställer störningsfri kritisk kommunikation i de allmänna kommunikationsnäten. De som gav utlåtanden såg inget behov av att beakta säkerhetsfrågor beträffande nätverksskivning av mobilnät i den nya versionen av föreskriften, eller så ansåg de att en allmän hänvisning till befintliga rekommendationer skulle vara tillräcklig.

Transport- och kommunikationsverket har ansett att det i och med kommunikationsnätens utveckling är nödvändigt att föreskriva mer detaljerat än tidigare om skyddet av gränssnitt. Föreskriften grundar sig i stor utsträckning på befintliga rekommendationer.

Filtrering av skadlig trafik i mobilnätets meddelandetjänster

I den tidigare föreskriften ingick inga särskilda skyldigheter beträffande informationssäkerheten i SMS- eller MMS-tjänster. Under de senaste åren har dock dessa tjänster i stor utsträckning använts vid spridning av skadliga program och bedrägerimeddelanden, vilket har krävt åtgärder av teleföretagen för att avhjälpa problemet.

[7] ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP), https://www.enisa.europa.eu/publications/7-steps-to-shore-up-bgp.

I enkäten som genomfördes sommaren 2022 före utarbetandet av föreskriften förhöll sig de som gav utlåtanden neutrala till att utvidga skyldigheten att filtrera skadlig trafik till SMS- och MMS-tjänster, eller så ansågs det vara nödvändigt.

De tekniska lösningar och färdigheter som används för filtrering varierar en aning bl.a. enligt huruvida det är fråga om en SMS- eller en MMS-tjänst. Transport- och kommunikationsverket anser att det är nödvändigt att utfärda föreskrifter i frågan för att säkerställa adekvata filtreringsfärdigheter. Som alternativa lösningar har ämbetsverket övervägt ett krav på förmåga att innehållsbaserat filtrera skadlig trafik för både SMS- och MMS-tjänster i alla fall samt ett alternativ där tillämpningen av detta krav skulle begränsas i MMS-tjänster som används i mindre utsträckning och där det inte finns lika etablerade lösningar för liknande filtrering som för SMS-tjänster. När man beaktar den ringa användningen av MMS-tjänster anser inte Transport- och kommunikationsverket att det är motiverat att utan undantag förutsätta en förmåga till innehållsbaserad filtrering i fråga om dessa tjänster, när man avväger de kostnader som detta förmodligen skulle orsaka i relation till alternativa metoder som kan användas för att ingripa i spridning av skadliga program eller bedrägerimeddelanden med hjälp av MMS-meddelanden. Därför har ämbetsverket i föreskriften valt en modell där ett teleföretag i vissa situationer kan använda andra metoder istället för innehållsbaserad filtrering.

Åtgärder för filtrering av e-posttrafik från konsumentabonnemang

Transport- och kommunikationsverket har bedömt huruvida filtreringsskyldigheten för obegränsad e-posttrafik, dvs. port 25, ska a) bevaras som den är, b) tas bort och filtreringsåtgärden avgörs enligt den s.k. *förordningen om öppet internet*[8] och 272 § i lagen om tjänster inom elektronisk kommunikation samt c) att ett undantag läggs till i filtreringsskyldigheten för situationer där konsumenten begär att filtreringsåtgärden avlägsnas.

Transport- och kommunikationsverket utredde hösten 2022 läget för begränsning av SMTP-trafik i internetaccesstjänster i övriga länder i Europa. På basis av icke-heltäckande uppgifter från andra tillsynsmyndigheter filtreras i synnerhet utgående e-posttrafik från konsumentabonnemang till port 25 i de flesta länder, men det finns även länder där denna trafik inte filtreras alls av de viktigaste operatörerna. I de fall där filtrering görs framkom det i regel samtidigt att konsumenten dock har möjlighet att begära att filtreringsåtgärden avlägsnas. I de övriga länderna baserar sig denna filtrering veterligen inte på en bindande föreskrift som i Finland.

Transport- och kommunikationsverket utfärdade år 2022 ett beslut som med avvikelse från föreskriften gällde motsvarande filtreringsåtgärd i vissa företagsabonnemang, för vilka föreskriften inte kräver filtrering.[9] I beslutet bedömdes huruvida ett teleföretag hade grund för att tillämpa begränsningen av e-posttrafik till kommunikationsport 25 som varit obligatorisk för konsumenter även på vissa företagsabonnemang. I den situation som bedömdes i beslutet fanns det inte tillräckliga grunder för detta, eftersom det var fråga om sådana andra än konsumentabonnemang som var avsedda för dataöverföring i mobilnätet och som hade en fast IP-adress. I beslutet togs inte ställning till huruvida begränsningen skulle ha varit motiverad i företagsabonnemang i andra situationer.

[8] Europaparlamentets och rådets förordning (EU) 2015/2120 om åtgärder rörande en öppen internetanslutning och om ändring av direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster och förordning (EU) nr 531/2012 om roaming i allmänna mobilnät i unionen.
[9] Begränsning av e-posttrafik från företagsabonnemang, dnr Traficom/9900/09.00.00/2021.

I enkäten som genomfördes sommaren 2022 före utarbetandet av föreskriften ansågs filtrering av obegränsad SMTP-trafik från konsumentabonnemang fortfarande nödvändig. Transport- och kommunikationsverket begärde synpunkter även på huruvida föreskriften borde utvecklas så att ett teleföretag på konsumentens begäran skulle ta bort begränsningen på abonnemanget. Två teleföretag som gav utlåtanden i frågan ansåg inte att detta var motiverat. I ett utlåtande lyftes fram att det inte skulle vara hanterings- eller kostnadsmässigt vettigt att göra separata konsumentabonnemang med egna regler för några användare.

Transport- och kommunikationsverket bedömde att det fortfarande är motiverat att bibehålla den principiella filtreringsskyldigheten för konsumentabonnemang i föreskriften för avvärjande av informationssäkerhetshot. Genom åtgärden ingriper man i hotet om skadlig trafik som orsakas av skadliga program som försöker skicka skräppost från terminalutrustning eller felaktigt konfigurerade e-postservrar. Ett avlägsnande av skyldigheten bedömdes öka mängden skräppost, även om spridningen av skräppost från konsumentabonnemang begränsas av den numera mer allmänna användningen av DKIM- och SPF-metoder samt användning av olika typer av ryktesbaserade system, som begränsar användningen av IP-adresser som konsumentabonnemang använder för sändning av e-post.

Beträffande bevarandet av skyldigheten ska uppmärksamhet ägnas även åt begränsningens inverkan på möjligheten att tillhandahålla e-postservrar från konsumentabonnemang. Bedömningen är att filtreringsåtgärden i konsumentanvändning mycket sällan orsakar betydande olägenheter för användaren, trots att den begränsar tillhandahållandet av e-postservrar med hjälp av abonnemang. Det är inte möjligt att exakt bedöma hur stor andel av konsumenterna som skulle vara villiga att använda en egen e-postserver i ett abonnemang i situationer där filtrering inte skulle vara i bruk. Man kan dock uppskatta att det skulle vara fråga om en rätt liten användargrupp, vilket det fåtal förfrågningar till Transport- och kommunikationsverket om de negativa effekterna av filtreringen i port 25 under de senaste åren också tyder på. Kunderna har dessutom typiskt tillgång till exempelvis abonnemang som är avsedda för företagsbruk och där filtreringsåtgärder inte används.

Om man i föreskriften skulle kräva att teleföretag på kundens begäran tar filtreringen ur bruk skulle det ge upphov till kostnader för företaget. Teleföretaget skulle i provisioneringsmiljön behöva skapa en möjlighet att ändra de filter som används per abonnemang. Beroende på typen av abonnemang är detta nödvändigtvis inte tekniskt sett rimligt att genomföra heller. Enligt de uppgifter som erhölls under arbetet i Transport- och kommunikationsverkets arbetsgrupp skulle detta vara en arbetskrävande förändring för teleföretagen. Ändringen skulle få kostnadseffekter som kunde drabba hela kundkretsen. Transport- och kommunikationsverket känner dock inte till några exakta uppgifter om de faktiska kostnaderna för företagen. Dessutom kan påpekas att det i en del andra länder redan verkar finnas en sådan här möjlighet till undantag. När man emellertid beaktar ovanstående som sagts om informationssäkerheten och begränsningarnas konsekvenser för kunderna verkar det motiverat att uppskatta att eventuella nackdelar med ändringen i princip är större än fördelarna. Saken kan utvärderas på nytt exempelvis i samband med följande uppdatering av föreskriften.

Begränsningar av tillämpningen för tjänster för förmedling av e-post och sekundära tjänster för förmedling av e-post

Transport- och kommunikationsverket bedömde huruvida tillämpningsbegränsningarna ska förbli som tidigare eller avlägsnas från föreskriften. Som ett resultat av bedömningen har tillämpningsbegränsningarna delvis avlägsnats från föreskriften som onödiga.

Beträffande filtreringsskyldigheten är det enligt ämbetsverkets bedömning för det första inte motiverat att utesluta inkommande trafik som äventyrar informationssäkerheten i system som används för produktion av sekundära tjänster för förmedling av e-post. Det är i princip motiverat att tillämpa filtreringsskyldigheten även på annan inkommande skadlig trafik. Redan den tidigare föreskriften gjorde det möjligt att avvika från detta genom att komma överens med kunden, vilket kommer att vara möjligt även framöver. För det andra är det motiverat att framöver tillämpa skyldigheten att filtrera utgående skadlig trafik i princip även på tjänster för förmedling av e-post, så att även informationssäkerheten i denna trafik säkerställs.

På basis av de uppgifter som Transport- och kommunikationsverket erhållit är också de filtreringar som används i tjänster för förmedling av e-post och sekundära tjänster för förmedling av e-post i de flesta fall redan för närvarande desamma som teleföretagen annars använder. Föreskriften lämnar i varje fall rum för möjligheten till tillämpning enligt med vilka metoder det är motiverat att filtrera skadlig trafik i olika typer av tjänster. Därför är det inte längre nödvändigt att i punkt 26 i denna föreskrift inkludera begränsningar av tillämpningsområdet som motsvarar den tidigare föreskriften.

Enligt denna och den tidigare föreskriften ska teleföretag som tillhandahåller e-posttjänster som primärt alternativ erbjuda kunderna en skyddad förbindelse mellan kunden och e-postlådan samt mellan kunden och e-postservern för utgående trafik. Denna skyldighet tillämpades enligt den tidigare föreskriften inte på tjänster för förmedling av e-post. Detta har i praktiken inneburit att man inte har behövt tillhandahålla en skyddad förbindelse till sådana användare av internetaccesstjänsten som är kunder hos en annan leverantör av e-posttjänster men som har önskat använda port 25 för sändning av e-post. I sådana fall har de i fråga om filtreringen i denna port (14.1 § i den tidigare föreskriften, punkt 21.1 i denna föreskrift) behövt använda en e-postserver för utgående SMTP-trafik som tillhandahålls av ett teleföretag som fungerar som tillhandahållare av internetaccesstjänsten. Användning av TLS-kryptering utan autentisering i port 25 är i sig tekniskt möjlig, även om tillhandahållandet av detta alternativ enligt Transport- och kommunikationsverkets uppfattning för närvarande varierar i praktiken. Tillhandahållandet av kryptering skulle stödja föreskriftens mål att främja informationssäkerheten i kommunikationstjänster och trygga den elektroniska kommunikationens konfidentialitet. Därför har det bedömts huruvida tillämpningsbegränsningen borde avlägsnas så att skydd av förbindelsen skulle erbjudas även vid användning av port 25 i tjänster för förmedling av e-post.

När en kund använder tjänster hos en annan e-posttjänsteleverantör med hjälp av en e-postapplikation i terminalutrustningen hindrar inte filtreringen i port 25 denna från att använda den egna e-postleverantörens server för sändning av e-post i till exempel port 587 eller 465. En kund som vill att kryptering används kan i detta fall hur som helst direkt använda den egna e-posttjänsteleverantörens server istället för en proxyserver, om det är möjligt att använda en annan port än port 25. Enligt Transport- och kommunikationsverkets uppfattning hindrar däremot filtreringen i port 25 i praktiken genomförande av en vanlig e-postserver med hjälp av ett konsumentabonnemang, om inte den egna internetaccesstjänstleverantörens SMTP-server används som proxyserver (relay) för sändning av meddelanden. Därför bedömer Transport- och kommunikationsverket att det är motiverat att framöver förutsätta att teleföretag tillhandahåller en möjlighet till kryptering av förbindelsen även vid användning av proxyservrar för e-post.

Detta bedöms orsaka endast mindre kostnader för ändringar i inställningarna för de tjänsteleverantörer som ännu inte erbjuder denna möjlighet.

Skyldigheter beträffande information till kunderna

Kapitel 6 om information till kunderna i den tidigare föreskriften har tagits bort från denna föreskrift. Transport- och kommunikationsverket bedömde att målen för skyldigheterna i fråga uppnås som sig bör redan genom att tillämpa bestämmelserna på lagens och förordningens nivå, varvid det inte finns något behov av att ålägga närmare bindande föreskrifter i frågan.

I statsrådets förordning om information som ska ges innan avtal om kommunikationstjänster ingås (96/2021) föreskrivs om lämnandet av uppgifter när tjänsteleverantörens åtgärder om informationssäkerheten är hotad eller när hot eller sårbarheter som gäller informationssäkerheten uppstår (1 § 6 punkten). Detta motsvarar väsentligt 21 § i den tidigare föreskriften som gällde allmänt givande av information om åtgärder i fråga om informationssäkerheten. Det som föreskrivs i statsrådets förordning kan dessutom bedömas omfatta även den särskilda skyldigheten att ge information om filtreringsprinciperna för e-posttjänster som det föreskrevs om i 23 § i den tidigare föreskriften. Dessutom ska information om behandlingen av förmedlingsuppgifter i anknytning till filtreringen ges med stöd av 138 § 2 mom. i lagen om tjänster inom elektronisk kommunikation. Beträffande praxis för administration av e-postadresser bedöms att lämnande av uppgifter inom ramarna för den tidigare skyldigheten numera hör till normala kundservicerutiner.

Den tidigare föreskriftens 22 § om särskild skyldighet att ge information om internetaccesstjänster gällde de informationssäkerhetsrisker som hänför sig till användningen av ett abonnemang och lämnandet av uppgifter om vilka åtgärder kunden använder i anknytning till dessa risker. Ett exempel som nämndes i motiveringspromemorian var tillhandahållande av internetaccesstjänster med hjälp av en okrypterad WLAN-förbindelse, varvid teleföretaget skulle underrätta kunden om de särskilda risker som kan förekomma då abonnemanget används för konfidentiell kommunikation. För närvarande erbjuds allmänt tillgängliga kommunikationstjänster veterligen inte med hjälp av WLAN-förbindelser i någon större utsträckning. Därtill begränsar den mer utbredda krypteringen av HTTP-trafik och användningen av VPN-anslutningar i viss mån de informationssäkerhetsrisker som orsakas av avsaknad av kryptering för WLAN-förbindelser. Såvitt en informationssäkerhetsrisk kan rikta sig mot ett teleföretag, finns det bestämmelser om anvisningar som teleföretaget ska ge användarna i 246 § 3 mom. i lagen om tjänster inom elektronisk kommunikation. Enlig den ska abonnenterna administrera utrustning och system som ansluts till ett allmänt kommunikationsnät i enlighet med teleföretagets anvisningar så att de inte äventyrar informationssäkerheten i det allmänna kommunikationsnätet och i de allmänna kommunikationstjänsterna. Därtill föreskrivs i 274 § 2 mom. i lagen om tjänster inom elektronisk kommunikation om teleföretagets skyldighet att informera om vilka skyddsåtgärder som kan vidtas, när teleföretaget informerar abonnenten eller användaren om en informationssäkerhetsincident eller hotet om en sådan som riktar sig mot teleföretagets tjänst.

Transport- och kommunikationsverket har ändrat största delen av innehållet i kapitel 6 i den tidigare föreskriften till rekommendationer i kapitel 7 i bilagan till denna motiveringspromemoria.

V. Beredning av föreskriften

Transport- och kommunikationsverket inledde beredningen av föreskriftsändringen genom att sommaren 2022 genomföra en enkät om erfarenheter och utvecklingsidéer bland teleföretag och allmänheten.[10] Enkäten besvarades av DNA Abp, Elisa Abp, Telia Finland Oyj, Suomen Erillisverkot Oy och Huawei Technologies Oy (Finland) Co. Ltd. samt en privatperson. Svaren utnyttjades i utarbetandet av utkastet till föreskrift.

I januari 2023 bad Transport- och kommunikationsverket teleföretagen att utse medlemmar till föreskriftsarbetsgruppen. Till arbetsgruppen anmälde sig och utsågs representanter för följande aktörer: Digita Oy, DNA Abp, Elisa Abp, FiCom ry, Finnet-liitto ry, Ikaalisten-Parkanon Puhelin, Karis Telefon Ab, Line Carrier Oy, Telia Finland Oyj, Telia Inmics-Nebula Oy och Ålands Telekommunikation Ab. Arbetsgruppen sammanträdde åtta gånger under 2023. I arbetsgruppens möten behandlades utkasten till föreskrift och motiveringspromemoria.

Remissbehandlingen ordnades […].

VI. Remissrespons

[Kompletteras under behandlingen]

VII. Ändringar och bedömning av föreskriftens konsekvenser

I detta kapitel beskrivs de viktigaste ändringarna som gjorts i föreskriften och deras effekter.

Kapitel 1 i föreskriften

- Föreskriftens mål beskrivs i fortsättningen endast i motiveringspromemorian.
- Föreskriftens tillämpningsområde har ändrats så att begränsningar av tillämpningen för tjänster för förmedling av e-post och sekundära tjänster för förmedling av e-post har raderats ur föreskriften. Dessutom utvidgades redan den tidigare föreskriftens innehåll att omfatta tillämpningsområdet för skyldighet att förhindra störningar till myndighetsnäten till att även omfatta en kommunikationstjänst i anslutning till myndighetskommunikation.
- I definitionerna har definitionen av skadlig trafik kompletterats så att den på ett tydligare sätt än tidigare omfattar samma situationer i vilka 272 § i lagen om tjänster inom elektronisk kommunikation möjliggör åtgärder för behandlingen av kommunikation för att genomföra informationssäkerheten.
- I stället för en öppen e-postserver ändrades begreppet som ska fastställas till en öppen proxyserver för e-post, så att definitionen motsvarar det begrepp som används i skyldigheterna i föreskriften.
- I definitionerna har definitionen av en textmeddelandetjänst och en tjänst för multimedia lagts till, vilka används i det nya kapitel 5.

[10] Uppdatering av föreskriften om televerksamhetens informationssäkerhet (67 A/2015 M): Enkät om erfarenheter och utvecklingsidéer, dnr Traficom/16241/09.09/2022 (på finska): https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=e80c3ac0-6941-4bba-bdcf-62c826646465&proposalLanguage=da4408c3-39e4-4f5a-84db-84481bafc744.

Kapitel 2 i föreskriften

- Punkten Hänsynstagande till informationssäkerheten har utvidgats jämfört med den tidigare föreskriften. De delområden som ska beaktas motsvarar den indelning av informationssäkerheten i åtta delområden som tillämpas i ENISAs riktlinjer. Varje delområde preciseras i nya punkter, där de säkerhetsmål som ENISA fastställt för respektive delområde har utnyttjats, dock med beaktande av att det delvis föreskrivs om säkerhetsmålen även i andra föreskrifter utfärdade av Transport- och kommunikationsverket. Bakgrunden till uppdateringen av föreskriften är i detta hänseende ett behov av att göra den aktuell samt beakta i synnerhet de nya arkitekturförändringarna och användningsfallen i fråga om 5G-näten.

  Även om man i föreskriften inte längre som sådan använder en indelning av terminologin enligt den tidigare föreskriften i administrativ informationssäkerhet, personalsäkerhet, maskinvaru-, programvaru- och telekommunikationssäkerhet, datamaterial- och driftsäkerhet samt fysisk säkerhet är tanken ändå att föreskriften fortfarande ska omfatta alla dessa delområden.

  Föreskriftens högre detaljnivå än tidigare orsakar dock aningen mer arbete för teleföretagen, i synnerhet om de är tvungna att införa nya åtgärder och dokumentera dem. Relativt sett är konsekvenserna störst för mindre teleföretag, där man tidigare inte nödvändigtvis har använt sig av ENISAs material i någon större utsträckning. Å andra sidan vägleder preciseringen av föreskriften på ett tydligare sätt än tidigare teleföretagen vid genomförandet av nödvändiga informationssäkerhetsåtgärder, vilket även i viss mån förenklar fastställandet av vilka åtgärder som behövs och därigenom tillämpningen av föreskriften.

  Ändringen bedöms klart förbättra informationssäkerheten, då föreskriften på ett tydligare sätt än tidigare ger vägledning för genomförande av närmare fastställda mål för informationssäkerheten. I genomförandet av informationssäkerhetsmålen å andra sidan är det möjligt att använda bl.a. de informationssäkerhetskontroller som ENISA fastställt och som är enkla att kombinera med skyldigheterna enligt föreskriften. Detta stöder även dokumentationen.

  Ändringen bidrar även till att öka effektiviteten och förutsägbarheten hos Transport- och kommunikationsverkets tillsyns- och kontrollverksamhet, då man i verkställandet av föreskriften kan stödja sig på ENISAs klart definierade informationssäkerhetsmål och -kontroller.

- Skyldigheten att spara dokumentation om riskbehandlingens resultat har förlängts till föregående tre behandlingsomgångar istället för en. Dokumentation om en behandlingsomgång enligt den tidigare bestämmelsen har inte varit tillräcklig för att kunna fastställa riskhanteringens kontinuitet. I standarden ISO/IEC 27005 gäller kravet två behandlingsomgångar. Eftersom lagring av resultat för fler behandlingsomgångar inte resulterar i väsentligt mer extra arbete, har kravet i föreskriften utvidgats till tre behandlingsomgångar.

- Som en särskilt viktig punkt i anknytning till underleverans och leveranskedjor har ombesörjande av informationssäkerhetsrisker lyfts upp på föreskriftsnivå. Även exempelvis upprätthållande av medvetenheten om hot har lyfts fram som en separat punkt i föreskriften.

- Förfaranden för efterlevnad av mobilnätstandarder har införts som ett nytt krav i föreskriften. Skyldigheten förutsätter att teleföretag inför förfaringssätt med hjälp

av vilka man säkerställer att de säkerhetsåtgärder som beskrivs i standarderna genomförs i teleföretagens 4G- och 5G-nät. Föreskriften ger dock möjlighet att låta bli att genomföra en funktion som beskrivs i standarderna om teleföretaget har en grundad anledning till det och riskerna hanteras på annat sätt. Detta gör det möjligt för teleföretagen att istället för att genomföra säkerhetsåtgärderna enligt standarderna alternativt fastställa och dokumentera ersättande åtgärder.

Skyldigheten bedöms inte i sig medföra några betydande merkostnader för teleföretag i mobilnätet, eftersom målet i varje fall är att iaktta standarderna i fråga vid upphandlingar och från tillverkarnas håll. Att beakta och eventuellt låta bil att genomföra förfaringssätten och säkerhetsfunktionerna samt dokumentera ersättande åtgärder ger dock upphov till en del kostnader. Skyldigheten att dokumentera förfarandena medför att teleföretag ska inkludera uppföljning av standarderna i fråga i sina dokumentationsprocesser och övriga processer, till exempel hanteringen av konfigurationer.

- Identifiering av kunder i syfte att ombesörja informationssäkerheten har införts som en ny punkt i föreskriften.

  Företag som följer bästa praxis inom området bedöms inte få några betydande merkostnader, eftersom det är fråga om åtgärder som det är skäl för varje teleföretag att även annars genomföra. Genom skyldigheten understryks dock behovet av ständig utveckling. Om företagets rutiner inte har varit på en tillräcklig nivå tidigare stöder en särskild skyldighet övervakningen av rutinerna och lyfter fram dessa företags behov av att utveckla sina rutiner.

- Punkten om skydd av hanteringsnät och hanteringsförbindelser har preciserats. Ett krav på utarbetande av verksamhetsprinciper och förfaranden samt bedömning och hantering av risker i anslutning till terminalutrustning som används för hanteringen har lagts till i punkten.

<u>Kapitel 3 i föreskriften</u>

- Den första underpunkten i punkten Förhindrande av och skydd mot störningar i gränssnitten har utvidgats så att den gäller förhindrande av störningar även i alla andra kommunikationsnät och inte endast i de allmänna kommunikationsnäten. Den andra underpunkten har utvidgats till tillämpningsgränssnitt och förtydligats så att skyldigheten gäller både kommunikationsnät och -tjänster.

- Punkten Skydd av IP-samtrafikgränssnitt och filtrering av trafiken har utvidgats jämfört med den tidigare föreskriften. Punkten behandlar i första hand tryggande av BGP-routingprotokollet som i den tidigare föreskriften gällde närmast ruttannonsering. Som delområden inom skyldigheterna har de viktigaste förfarandena utifrån ENISAs rekommendationer lyfts fram.

  Föreskriftens högre detaljnivå än tidigare medför delvis extra arbete för teleföretagen. Största delen av skyldigheterna har redan åtminstone i viss mån beaktats, och föreskriften närmast stärker redan befintlig praxis. Föreskriftens högre detaljnivå än tidigare leder teleföretagen till att genomföra nödvändiga skydds- och filtreringsåtgärder i anknytning till BGP-routing.

  Ändringarna bedöms ha en stärkande och upprätthållande effekt på BGP-routingprotokollets säkerhet. Eftersom de mest centrala säkerhetsegenskaperna utifrån ENISAs rekommendationer har inkluderats som delområden i föreskriften, anses

detta även underlätta verkställandet av förordningen. Utgångspunkten i ENISAs rekommendationer underlättar även Transport- och kommunikationsverkets övervakning samt uppföljningen och utvecklingen av säkerhetsegenskaper i anknytning till BGP-routingprotokollet.

- En ny skyldighet beträffande skydd av gränssnitt i mobilnätet har lagts till i föreskriften. Mobilnätsgenerationernas livscykel är mycket lång, och fortfarande används exempelvis signalsystemet SS7, som ursprungligen skapades på 1970-talet och som en gång i tiden utvecklades för en mycket annorlunda hotmiljö. Man har senare försökt förebygga säkerhetsbristerna i signaleringsprotokollen med hjälp av anvisningar och rekommendationer för att åtgärda svagheterna.

  Skyldigheten bedöms inte medföra några extra kostnader för teleföretagen, om bästa praxis och rekommendationerna inom området redan iakttas i teleföretagets förfaranden. I och med arkitekturförändringarna i 5G-näten blir även skyddet av olika tillämpningsgränssnitt ännu viktigare, och de nya gränssnitt som i synnerhet ska beaktas är säkerheten i centrala funktionaliteter, såsom nätverksskivning och Edge Computing. Beträffande nätverksskivning är det viktigt att obehörig åtkomst till både nätverksskivans resurser och hanteringsgränssnitt förhindras. Dessutom är det viktigt att åtkomstkontrollen i radiogränssnitt stärks efter behov genom att bekräfta skivspecifik åtkomst. Enligt bästa praxis bedöms inte skyddet av hanterings- och radiogränssnitt medföra några extra kostnader för teleföretagen.

Kapitel 5 i föreskriften

- En ny punkt som lagts till i föreskriften är filtrering av text- och multimediatrafik. Skyldigheten bedöms i regel inte förutsätta några betydande nya investeringar av teleföretagen.

Kapitel 6 i föreskriften

- Begränsningarna av tillämpningsområdet för tjänster för förmedling av e-post och sekundära tjänster för förmedling av e-post har avlägsnats från föreskriften som onödiga. Ändringarna främjar informationssäkerheten, men bedöms inte ha några stora effekter på teleföretagens verksamhet. Beroende på teleföretagets rutiner förutsätter de inte nödvändigtvis några ändringar i tidigare rutiner. I en del fall kan det vara nödvändigt att göra ändringar i e-posttjänstens inställningar.

Avlägsnade skyldigheter

- Kapitel 6 om information till kunderna i den tidigare föreskriften har tagits bort (se Andra alternativ för verkställandet). De frågor som behandlats i kapitlet har flyttats till bilagan till denna motiveringspromemoria, som också i övrigt har kompletterats.

DETALJMOTIVERING OCH TILLÄMPNINGSANVISNINGAR

Kapitel 1 Tillämpningsområde och definitioner

Detta kapitel behandlar föreskriftens kapitel 1, dvs. föreskriftens tillämpningsområde och definitioner.

1. Tillämpningsområde

1.1 Föreskriftens allmänna tillämpningsområde

Föreskriften gäller allmän televerksamhet. Föreskriften är därmed förpliktande för alla teleföretag oberoende av vilken typ av tjänst de tillhandahåller. Föreskriften tillämpas också på televerksamhet som är av ringa betydelse och som inte omfattas av den anmälningsplikt enligt 4 § i lagen om tjänster inom elektronisk kommunikation som gäller bedrivande av verksamhet.

Enligt 3 § 1 mom. 27 punkten i lagen om tjänster inom elektronisk kommunikation avser teleföretag ”en aktör som tillhandahåller nättjänster eller kommunikationstjänster för en grupp av användare som inte har avgränsats på förhand”.

Nättjänsten definieras också i 3 § 1 mom. i lagen, och med den avses en tjänst som tillhandahålls av ett teleföretag för att ett kommunikationsnät som det äger eller på någon annan grund förfogar över ska kunna användas för överföring och distribution av meddelanden. Teleföretag som tillhandahåller nättjänster kallas även *nätföretag* i lagen om tjänster inom elektronisk kommunikation. Enligt lagen är *kommunikationsnät* ett system som består av sammankopplade ledningar och av anordningar, och som är avsett för överföring eller distribution av meddelanden via ledning, med radiovågor eller på något annat elektromagnetiskt sätt. Sådana kommunikationsnät som används för att tillhandahålla kommunikationstjänster till en grupp av användare som inte har avgränsats på förhand är enligt lag *allmänna kommunikationsnät*. Sådana kommunikationsnät som huvudsakligen används för överföring eller sändning av televisions- och radioprogramutbud eller annat material som förmedlas i samma form till alla mottagare är i sin tur enligt lagen *masskommunikationsnät*.

Med *kommunikationstjänst* avses enligt 3 § 37 punkten i lagen om tjänster inom elektronisk kommunikation "en tjänst som helt eller huvudsakligen utgörs av överföring av meddelanden i kommunikationsnät samt överförings- och sändningstjänster i masskommunikationsnät och interpersonella kommunikationstjänster" (lagen 1207/2020). Föreskriften tillämpas på såväl nummerbaserade som nummeroberoende interpersonella kommunikationstjänster.

Kraven i föreskriften är indelade i sex sakhelheter:

- I kapitel 2 fastställs de allmänna kraven på informationssäkerhet i alla kommunikationsnät och -tjänster.
- I kapitel 3 behandlas de åtgärder som ska vidtas i fråga om informationssäkerheten i samtrafik-, tillämpnings- och kundgränssnitt.
- I kapitel 4 fastställs särskilda krav på att sörja för informationssäkerheten i internetaccesstjänster.
- I kapitel 5 fastställs särskilda krav på att sörja för informationssäkerheten i SMS- och MMS-meddelandetjänster.
- I kapitel 6 behandlas de särskilda kraven för e-posttjänster.

Föreskriften *tillämpas inte på annan än allmän televerksamhet*. Allmän televerksamhet är inte nät- eller kommunikationstjänster eller innehållstjänster som tillhandahålls en grupp användare som har avgränsats på förhand. Innehållstjänster som faller utanför tillämpningsområdet är t.ex. webbsidors innehåll, diskussionsforum samt innehållet i televisions- och radioprogram.

Föreskriften gäller således inte andra *kommunikationsförmedlare* än teleföretag, dvs. *sammanslutningsabonnenter* och *andra kommunikationsförmedlare*.[11] Föreskriften ålägger inte till exempel sammanslutningsabonnenter skyldigheter. Föreskriften lämpar sig inte för hantering av ett företags eller en sammanslutnings interna kommunikationsnät, eftersom gruppen av användare i det fallet har avgränsats på förhand och det inte är fråga om allmän televerksamhet. Sammanslutningsabonnenter är sådana *abonnenter* som avses i lagen om tjänster inom elektronisk kommunikation. Även om teleföretaget som tillhandahåller tjänsten inte svarar för sammanslutningens interna kommunikationsnät eller -tjänst, är teleföretaget ansvarigt för den tjänst företaget erbjuder abonnenten.

1.2 Tillämpning av föreskriften på myndighetsnät och kommunikationstjänster i anslutning till myndighetskommunikation

Även om föreskriften annars tillämpas endast på televerksamhet, tillämpas punkt 15.1 i föreskriften på myndighetsnät och myndighetstjänster i anslutning till myndighetskommunikation när dessa har sammankopplats med ett allmänt kommunikationsnät eller en allmänt tillgänglig kommunikationstjänst, det vill säga ett teleföretags nät eller tjänst. Till övriga delar gäller föreskriften inte myndighetsnät.

Med *myndighetsnät* avses enligt 3 § 39 a punkten i lagen om tjänster inom elektronisk kommunikation kommunikationsnät som byggts för myndighetsuppgifter som avser statens ledning och säkerhet, försvaret, den allmänna ordningen och säkerheten, gränssäkerheten, räddningsverksamheten, sjöräddningen, nödcentralsverksamheten, invandringen, jourverksamheten inom social- och hälsovården, spårtrafiksäkerheten och befolkningsskyddet (lagen 52/2019). Ett exempel på ett myndighetsnät är VIRVE.

Med *kommunikationstjänst i anslutning till myndighetskommunikation* avses en tjänst som tillhandahålls av en i 3 § 39 c-punkten i lagen om tjänster inom elektronisk kommunikation avsedd *tillhandahållare av kommunikationstjänst med anknytning till myndighetskommunikation*, det vill säga en informations- och kommunikationsteknisk tjänst för myndigheternas tidskritiska mobilkommunikationstjänst med bredband.[12]

Föreskriften ålägger inga skyldigheter för sådana lokala nät som inte är allmän televerksamhet. Beroende på genomförandesättet kan även dessa omfattas av skyldigheter som föreskrivs i lagen tjänster inom elektronisk kommunikation. Om ett lokalt nät har

[11] Enligt 3 § 36 punkten i lagen om tjänster inom elektronisk kommunikation avses med kommunikationsförmedlare ett teleföretag, en sammanslutningsabonnent och en sådan annan aktör som förmedlar elektronisk kommunikation för andra än personliga eller med sådana jämförbara sedvanliga privata ändamål (nedan annan kommunikationsförmedlare). Med *sammanslutningsabonnent* avses enligt 3 § 41 punkten i lagen om tjänster inom elektronisk kommunikation ett företag eller en organisation som abonnerar på kommunikationstjänster eller mervärdestjänster och som i sitt kommunikationsnät behandlar meddelanden från användare samt förmedlingsuppgifter och lokaliseringsuppgifter.

[12] Föreskriften tillämpas i enlighet med dess allmänna tillämpningsområde även på nättjänster med anknytning till myndighetskommunikation och som betraktas som en del av den allmänna televerksamheten (RP 226/2018 rd, s. 49).

sammankopplats med ett allmänt kommunikationsnät ska man även i planeringen och användningen av det lokala nätet sörja för informationssäkerheten.[13]

2. Definitioner

I detta kapitel beskrivs de definitioner som används i föreskriften. I föreskriften omdefinieras inte de begrepp som definierats i lagen om tjänster inom elektronisk kommunikation. Definitionerna har utarbetats så att de inte strider mot definitionerna i lagen.

2.1 Kundgränssnitt

Med kundgränssnitt avses i denna föreskrift ett gränssnitt genom vilket ett kommunikationsnät, en terminalutrustning eller en applikation för teleföretagets kund kopplas till det allmänna kommunikationsnätet. Kundens terminalutrustning omfattar t.ex. modem, switchar och datorer som en beställare eller en användare äger och förfogar över. För denna typ av gränssnitt används på engelska benämningen User to Network Interface (UNI-gränssnitt).

2.2 Öppen proxyserver för e-post

Med öppen proxyserver för e-post avses ett sådant meddelandeförmedlingssystem för e-post som tredje part obehörigt kan använda för förmedling av e-postmeddelanden. Med förmedlingssystem avses i föreskriften t.ex. en e-postserver, www-proxyserver eller programvara som installeras i en www-server och används för förmedling av e-postmeddelanden.

2.3 Skadlig trafik och skräppost

Med skadlig trafik avses i föreskriften elektroniska meddelanden som utgör ett hot mot informationssäkerheten i kommunikationsnäten eller mot i dessa anknutna tjänster och datasystem, mot vilka åtgärder kan riktas på det sätt som avses i 272 § 1 mom. 2 punkten i lagen om tjänster inom elektronisk kommunikation för att trygga kommunikationsmöjligheterna för den som sänder eller tar emot meddelanden, eller meddelanden via kommunikationstjänsterna används för sådana omfattande förberedelser för betalningsbedrägeri som nämns i 37 kap. 11 § i strafflagen. Begreppet används bl.a. i de punkter i föreskriften som gäller textmeddelande-, multimedie- samt e-posttjänster och där det föreskrivs om skyldigheter som gäller filtrering av skadlig trafik. Tanken är att begreppet ska omfatta alla de situationer där det med stöd av 272 § i lagen om tjänster inom elektronisk kommunikation är möjligt att behandla meddelanden och förmedlingsuppgifter för att sörja för informationssäkerheten.

Med informationssäkerhet avses administrativa och tekniska åtgärder genom vilka det säkerställs att information är tillgänglig endast för dem som har rätt att använda den, att informationen inte kan ändras av andra än dem som har rätt till detta samt att informationen och informationssystemen kan utnyttjas av dem som har rätt att använda informationen och systemen. Ett elektroniskt meddelande kan beroende på fallet avse t.ex. ett IP-paket, ett e-postmeddelande eller ett SMS-meddelande, eller styrtrafik mellan nätets element.

[13] Transport- och kommunikationsverket: Ohje paikallisten matkaviestinverkkojen kyberturvallisuudesta ja riskienhallinnasta. Traficoms forskningsrapporter och utredningar, 8/2023, s. 19–20, https://www.kybertur-vallisuuskeskus.fi/fi/julkaisut/ohje-paikallisten-matkaviestinverkkojen-kyberturvallisuudesta-ja-riskienhal-linnasta.

Trafik som orsakas av blockeringsattacker, skräppost eller spridning av nätmaskar är därför exempel på skadlig trafik. Skadligheten i e-posttrafik ska granskas ur både tjänsteleverantörens och kundens synvinkel. Det innebär i praktiken t.ex. att säkerställandet av tillgängligheten av en kommunikationstjänst kan förutsätta åtgärder såväl för att se till att den tjänst tjänsteleverantören tillhandahåller kan förmedlas som att nivån på den service som erbjuds användaren upprätthålls. Vilken typ av skadlig trafik som ska avvärjas beror på den skyldighet som tillämpas och på tillämpningssituationen (såsom vilken kommunikationstjänst som det är fråga om).

2.4 Filtrering

Med filtrering avses förhindrande eller begränsning av sådan skadlig trafik som definieras ovan. Filtrering kan innebära t.ex. att internettrafik som utgår från en kundanslutning och nyttjar förfalskade källadresser förkastas, att kapacitet av en viss typ av internettrafik begränsas för en enskild anslutning eller på basis av det tillämpningsprotokoll som använts i trafikeringen, eller att förhindra förmedling eller mottagande av e-postmeddelanden.

Med filtrering avses också avlägsnande av sådana skadliga datorprogram ur meddelandena som kan äventyra informationssäkerheten, dvs. exempelvis avlägsnande av skadliga program ur e-postmeddelanden.

Därutöver kan filtrering avse även andra åtgärder av teknisk karaktär för att hantera trafik som äventyrar informationssäkerheten.

2.5 E-posttjänster

Med e-posttjänst avses en tjänst för sändning, förmedling eller mottagning av e-postmeddelanden som utnyttjar domännamnssystemet, dvs. en DNS-tjänst, för att förmedla meddelanden. Principerna för en e-posttjänst, skilda funktioner och de protokoll som används mellan funktionerna finns presenterade i figur 1.

Med tjänst för sändning av e-post avses en tjänst, där kunden sänder ett meddelande via tjänsteleverantörens e-postserver för utgående trafik (MSA, Message Submission Agent). Med tjänst för förmedling av e-post avses en tjänst, där e-postmeddelandet tas emot, (hanteras) och sänds vidare till ett med kunden överenskommet mål. Med tjänst för mottagning av e-post avses en tjänst, där kundens e-postmeddelande tas emot av en e-postserver för inkommande trafik (MDA, Message Delivery Agent) och levereras till kundens e-postlåda.

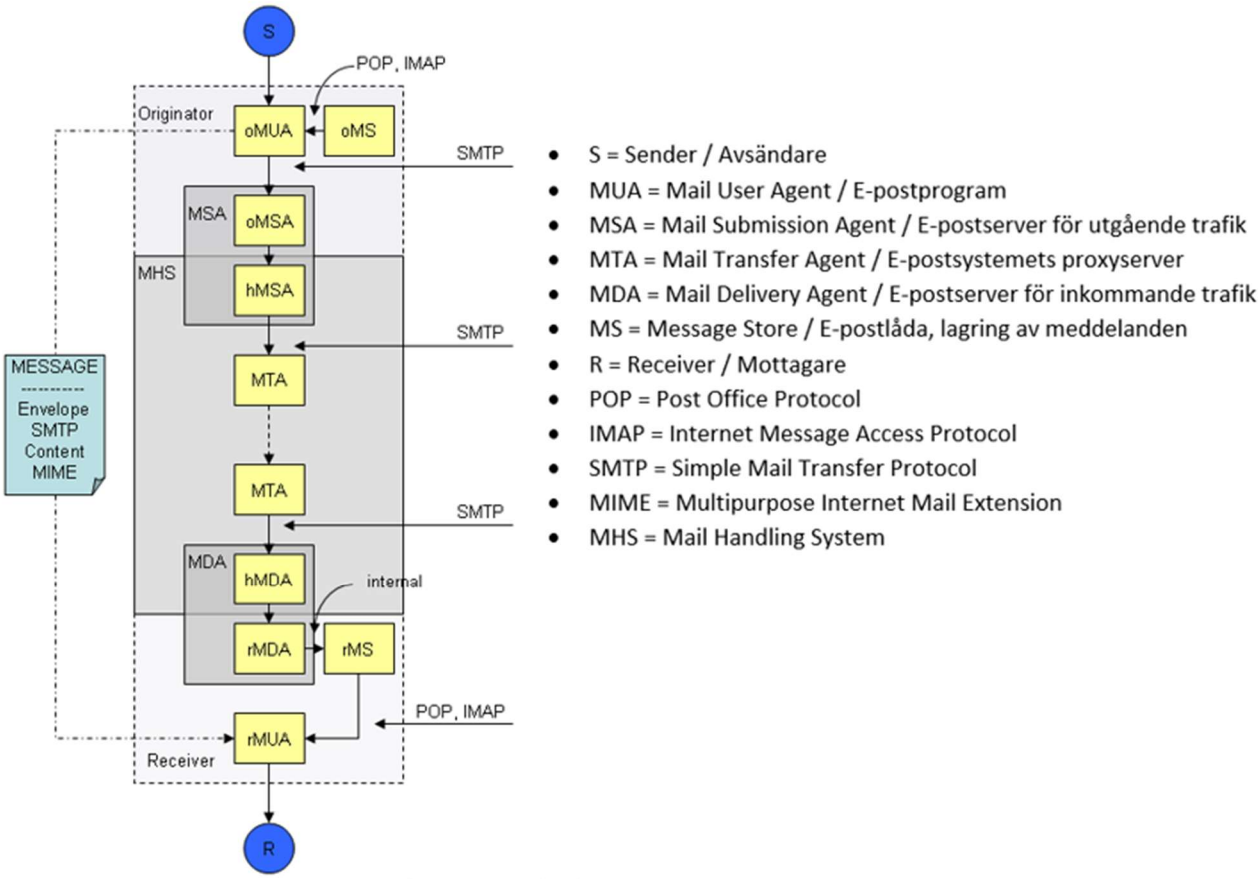

Bild 1. Principen för en e-posttjänst.

Med utgående e-posttrafik avses e-postmeddelanden som sänds av kunderna, och förmedlas via tjänsteleverantörens e-postservrar för utgående trafik (MSA, Message Submission Agent) till e-postsystemets proxyservrar (MTA, Message Transfer Agent).

Med inkommande e-posttrafik avses i sin tur e-postmeddelanden som sänds till tjänsteleverantörens kunder, och förmedlas via tjänsteleverantörens e-postservrar för inkommande trafik (MDA, Message Delivery Agent) till kundernas e-postlådor (MS, Mail Server).

Föreskriftens tillämpningsområde omfattar även *tjänster för förmedling av e-post* och *sekundära tjänster för förmedling av e-post*, vilka inte har definierats separat i föreskriften.[14]

Med *tjänster för förmedling av e-post* avses tjänster som en leverantör av e-posttjänster tillhandahåller genom att förmedla eller omdirigera meddelanden via sina egna e-postservrar (s.k. tjänster för omdirigering av meddelanden).

Skyldigheterna som gäller e-post tillämpas även på sekundära tjänster för förmedling av e-post som avser servrar för förmedling av e-post som säkerställer kundens egen e-posttjänst. I tjänsten har kundens e-postserver eller e-postservrar definierats som pri-

[14] Se punkten Andra alternativ för verkställandet om de ändringar som gjorts i denna föreskrift beträffande tillämpningsområdet för vissa skyldigheter.

mär mx-post eller primära mx-poster. Då förmedlas inkommande e-posttrafik till kunden via e-posttjänsteleverantörens sekundära proxyservrar endast i de fall då kundens egna servrar inte är tillgängliga. De skyldigheter som avser filtrering av inkommande e-posttrafik gäller i princip även sådana tjänster, men föreskriften ger möjlighet att avtala på annat sätt i frågan med kunden.

2.6 Komponent i kommunikationsnätet eller -tjänsten

Med kommunikationsnätets eller -tjänstens komponent avses ett nätelement, instrument eller informationssystem som kommunikationsnätet eller -tjänsten består av eller som det utnyttjar. Begreppet används i flera av Transport- och kommunikationsverkets föreskrifter.

Komponenter i kommunikationsnätet eller -tjänsten är t.ex. mobilstationer, basstationens kontrollenheter, basstationer, textmeddelandecentraler, bredbandskoncentratorer, namnservrar, servrar som svarar för nätets åtkomsthantering, switchar, routrar, SIP-applikationsservrar eller komponenter i intelligenta nät. Med en komponent i kommunikationsnät eller -tjänst avses inte transmissionsvägar eller delar av nätelement eller utrustning, såsom mobiltelefonväxlars processorenheter. Till komponenterna hör inte heller teleterminalutrustningar.

En komponent i kommunikationsnät eller -tjänster kan även genomföras i en virtualiseringsmiljö (se punkt 6.6 i motiveringspromemorian).

2.7 Samtrafikgränssnitt

Med samtrafikgränssnitt avses i denna föreskrift det gränssnitt där teleföretagens kommunikationsnät eller -tjänster kopplas samman. För denna typ av gränssnitt används på engelska benämningen Network to Network Interface (NNI-gränssnitt).

2.8 Textmeddelandetjänster och multimediemeddelandetjänster

Med *textmeddelandetjänst* avses i denna föreskrift en förmedlingstjänst för SMS-meddelanden, dvs. korta meddelanden som innehåller alfanumeriska tecken och specialtecken eller korta meddelanden i binärform genom förmedling via mobilnätets meddelandecentraler.

Med *multimediemeddelandetjänst* avses i föreskriften i sin tur en förmedlingstjänst av MMS-meddelanden, dvs. korta meddelanden som innehåller multimedia såsom bilder, ljud, videor och redigerad text via mobilnätets centraler för multimediemeddelanden.

2 kap. Allmänna krav på informationssäkerhet

Detta kapitel behandlar de krav i föreskriftens kapitel 2 som gäller ett teleföretags alla kommunikationsnät och -tjänster. Dessutom innehåller punkt 10 i föreskriften särskilda krav på teleföretag i mobilnät.

3. Hänsynstagande till informationssäkerheten

3.1 Delområden av informationssäkerheten

Informationssäkerheten utgör en viktig del av kvaliteten på de kommunikationsnät och -tjänster som teleföretaget tillhandahåller. Beaktande av informationssäkerhetens olika

delområden i televerksamhet är viktigt i alla faser av livscykeln för de kommunikationsnät och -tjänster som tillhandahålls: när de planeras, genomförs, underhålls och tas ur bruk. För att informationssäkerheten ska ombesörjas rutinmässigt varje dag, är det motiverat att förutsätta att teleföretaget fastställer processer och förfaranden för att genomföra informationssäkerheten.

Det finns flera olika faktorer som ska beaktas vid genomförandet av informationssäkerheten och i de dokument som beskriver det. I punkt 3.1 i föreskriften uppräknas de sakområden som ska beaktas och som motsvarar den indelning i åtta delområden (security domain) som följts i ENISAs riktlinjer för informationssäkerhetsåtgärder enligt teledirektivet.[15] Delområden som ska beaktas är:

1) informationssäkerhet och riskhantering,
2) personalsäkerhet,
3) säkerhet inom informationssystem och telekommunikationsområdet samt fysisk säkerhet,
4) informationssäker funktion och ändringshantering,
5) upptäckt och hantering av situationer som hotar eller stör informationssäkerheten,
6) driftskontinuitetshantering,
7) observation, testning och bedömning av informationssäkerheten, och
8) medvetenheten om hot samt information till abonnenter och användare.

Närmare minimikrav ställs för de olika delområdena i punkterna 4–9 nedan, där man i sin tur har använt de säkerhetsmål som ENISA fastställt för respektive delområde (security objective). Krav relaterade till delområdena ställs också i andra föreskrifter av Transport- och kommunikationsverket, och denna föreskrift ålägger inte detaljerade skyldigheter för alla delområden. Närmare krav relaterade till delområdena 5–6 samt delvis delområdena 7 och 8 ställs i huvudsak i föreskriften om störningar inom televerksamheten, som innehåller krav på bland annat upptäckt av och återhämtningsförfaranden vid informationssäkerhetskränkningar liksom anmälningar om fall av informationssäkerhetskränkningar. Delområde 5 omfattar förfaranden för hantering av informationssäkerhetskränkningar, upptäckt av informationssäkerhetskränkningar samt behandling av anmälningar om fall av informationssäkerhetskränkningar.[16] Delområde 6 avser i sin tur säkerställande av televerksamhetens kontinuitet i olika allvarliga störningssituationer, vilket omfattar till exempel förfaranden för återställande av verksamheten i allvarliga störningssituationer och säkerhetskopiering.[17] Den upptäckt som avses i delområde 7 omfattar utöver det som nämns i punkt 8 i föreskriften även övervakning av händelser som är viktiga med tanke på informationssäkerheten i synnerhet med hjälp av loggning.[18] Delområde 8 omfattar, förutom upprätthållande av teleföretagets hotmedvetenhet som behandlas i föreskriften, information till abonnenter och användare om informationssäkerhetshot, så att de kan ta i bruk behövliga skyddsmetoder och på så sätt även främja informationssäkerheten i kommunikationsnäten och -tjänsterna.[19]

[15] ENISA Guideline on Security Measures under the EECC, 4th Edition, July 2021 (nedan även ENISA GL).
[16] ENISA GL, SO18–SO20. Delområde 5 omfattar bland annat en samordnad första åtgärdsfunktion vid eventuella informationssäkerhetskränkningar, upprätthållandet av en kontaktpunkt för anmälningar samt abusefunktioner, det vill säga en funktion som är avsedd som kontaktpunkt och servicepunkt vid fall relaterade till kunder och externa intressentgrupper i samband med tillhandahållande av internettjänster.
[17] ENISA GL, SO21–SO22.
[18] ENISA GL, SO23.
[19] ENISA GL, SO29.

Rekommendationer om detta delområde relaterade till information till abonnenter och användare ges i punkt 7 i bilagan till denna motiveringspromemoria7.

I föreskriften uppställs de viktigaste informationssäkerhetsmålen och -åtgärderna för de flesta olika delområdena inom informationssäkerheten, men i princip ställs inga detaljerade krav på hur eller genom vilka informationssäkerhetsåtgärder (kontroller) som dessa olika helheter exakt ska beaktas i olika situationer. Vilka åtgärder för informationssäkerheten som är ändamålsenliga varierar i viss mån enligt teleföretag, bl.a. utifrån verksamhetens omfattning samt vilka nät och tjänster som tillhandahålls och de olika hoten i anknytning till dem. 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 (lagen om tjänster inom elektronisk kommunikation 243.3 §)

ENISAs matris[20] om 5G-informationssäkerhetsåtgärder innehåller både allmänna kontroller, som lämpar sig för all televerksamhet och som grundar sig på bland annat standardserien ISO/IEC 27000, och teknikspecifika kontroller, som grundar sig på bland annat 3GPP:s standard TS 33.501 i fråga om 5G-nät. Matrisen kan också utnyttjas för att uppfylla skyldigheterna i föreskriften. Föreskriftens minimikrav i anknytning till sakhelheterna har behandlats även i andra av Transport- och kommunikationsverket utfärdade föreskrifter eller på andra ställen i lagstiftningen, varför dessutom även teleföretagsspecifika krav som beror på avtal kan rikta sig till ombesörjandet av informationssäkerheten inom televerksamhet. Det väsentliga i punkt 3.1 i föreskriften är att teleföretaget ska identifiera de krav som gäller för dess verksamhet samt de förfaranden som ska tillämpas för att kraven ska uppfyllas. Istället för de informationssäkerhetskontroller som nämns som exempel i denna motiveringspromemoria är det möjligt att även använda andra lika effektiva åtgärder.

3.2 Informationssäkerhetsdokument

Punkt 3.2 i föreskriften förutsätter att teleföretaget har dokument om hur det i sin verksamhet genomför de allmänna kraven på informationssäkerhet enligt kapitel 2 i föreskriften. Dokumenten skapar en grund för systematisk utveckling och hantering av informationssäkerheten samt hjälper till att rikta investeringar till åtgärder för informationssäkerheten. Utifrån dokumentationen kan också Transport- och kommunikationsverket vid behov verifiera att teleföretaget iakttar sina skyldigheter att sörja för informationssäkerheten.

Föreskriften fastställer inte vilka alla olika dokument företaget ska ha, utan företaget får själv bedöma det. Det viktiga är att dokumentationen är aktuell och att man utifrån den kan konstatera att alla delområden av informationssäkerheten som omfattas av dokumentationsskyldigheten och närmare skyldigheter har beaktats i teleföretagets verksamhet.

4. Hantering av informationssäkerhet och risker

4.1 Informationssäkerhetspolicy och verksamhetsprinciper

Punkt 4.1.1 i föreskriften förutsätter att teleföretaget upprättar lämpliga styrdokument för informationssäkerhet, vilka är en informationssäkerhetspolicy och de verksamhetsprinciper som preciserar den. Genom informationssäkerhetspolicyn förbinder sig teleföretagets högsta ledning till att genomföra informationssäkerheten samt fastställer viljan

[20] ENISA 5G Security Controls Matrix, May 24, 2023, https://www.enisa.europa.eu/publications/5g-security-controls-matrix.

och principerna för att säkerställa informationssäkerheten för komponenterna i kommunikationsnäten och -tjänsterna samt för övriga objekt i anknytning till televerksamheten som ska skyddas. Vid upprättandet av styrdokumenten för informationssäkerheten kan teleföretaget stödja sig på exempelvis allmänt tillgängliga informationssäkerhetsstandarder eller ENISAs rekommendationer.[21] Krav för informationssäkerhetspolicyn och allmänt för systemet för hantering av informationssäkerheten har beskrivits även i exempelvis standarden ISO/IEC 27001.

Föreskriften förutsätter (punkt 4.1.1 och delvis punkt 3.2) att teleföretaget regelbundet granskar och vid behov upprätthåller (uppdaterar) sin informationssäkerhetspolicy samt de verksamhetsprinciperna för verkställande. Kontrollen ska enligt föreskriften uppmärksamma förändringar i verksamhetsmiljön, upptäckta avvikelser, övningar och förutsägbara förändringar i hotmiljön för informationssäkerheten. Vid bedömningen av eventuella avvikelser som upptäckts och som förutsätter ändringar i informationssäkerhetspolicyn eller verksamhetsprinciperna är det bra att i praktiken beakta om det är fråga om ett avsiktligt brott eller om avvikelsen beror på till exempel brist på utbildning, eftersom detta påverkar vilka praktiska åtgärder det är rimligt för teleföretaget att genomföra med anledning av fallet.

4.2 Risker

En risk är en kombination av en negativ omständighets eller händelses sannolikhet och konsekvenser.[22] Med informationssäkerhetsrisker avses i föreskriften en sådan oavsiktlig eller avsiktlig faktor som äventyrar televerksamhetens konfidentialitet, integritet eller tillgänglighet. En informationssäkerhetsrisk skiljer sig från ett informationssäkerhetshot i det att dess sannolikhet och konsekvenser har bedömts.

Informationssäkerhetsrisker kan t.ex. orsakas av:

- mänskliga misstag
- brister i eller underlåtenhet att iaktta instruktioner till personalen
- stölder eller skadegörelser
- fel eller funktionsstörningar i apparater, system eller program
- spridning av skadliga program
- förstöring av datamaterial
- eldsvåda eller översvämning
- fel och försummelser begångna av en underleverantör eller en aktör som ingår i samarbetsnätverket.

Med riskhantering avses en process som syftar till att identifiera risker, minska sannolikheten för risker och/eller konsekvenser av risker till en godtagbar nivå och bibehålla den uppnådda nivån. Syftet med riskhanteringen är att skydda organisationen och dess förmåga att utföra sina funktioner med beaktande av ekonomiska omständigheter.

Genom kraven på riskhanteringen strävar man efter att säkerställa att teleföretaget är medvetet om följderna om riskerna realiseras och huruvida de riskminskande åtgärderna är tillräckliga. Målet med riskhanteringen är bland annat att:

- snabba upp återhämtningen efter informationssäkerhetsproblem i televerksamheten
- minska kostnader och skador som förorsakas av informationssäkerhetsproblem
- rikta investeringar som förbättrar informationssäkerheten i televerksamheten
- förbättra televerksamhetens kvalitet och produktivitet

[21] T.ex. ENISA GL ja ENISA 5G Supplement to the Guideline on Security Measures under the EECC, 2nd Edition, July 2021.
[22] Ordlista om övergripande säkerhet, TSK 50, Helsingfors 2017.

- ekonomiskt optimera de risker som hänför sig till televerksamheten
- förebygga riskerna mot televerksamheten.

I 35 kap. i lagen om tjänster inom elektronisk kommunikation föreskrivs om teleföretagens beredskapsskyldighet.

Riskidentifiering och riskhantering

Punkt 4.1.2 i föreskriften förutsätter att teleföretaget ska identifiera och hantera riskerna i sin verksamhet och för verksamhetens kontinuitet. Riskhantering innebär att teleföretaget bedömer informationssäkerhetsriskerna, det vill säga genomför ändamålsenliga riskkontroller och godkänner eventuella kvarstående risker, samtidigt som företaget säkerställer att upprepade bedömningar ger jämförbara resultat. Som ett resultat av hanteringen fastställer teleföretaget en godtagbar risknivå för sin verksamhet och genomför nivån med ändamålsenliga metoder (ofta genom s.k. kontroller, dvs. genom olika risklindrande åtgärder eller åtgärder som minskar realisering av riskerna). I praktiken ska företaget fastställa ansvar och tidsplaner för riskhanteringen. Dessutom ska en lämplig ägare av riskerna utses som granskar och godkänner de kvarstående riskerna. Fullmakt att godkänna de kvarstående riskerna ska ges på teleföretagets organisationsnivå, i enlighet med den godkända informationssäkerhetspolicyn.[23]

Föreskriften ålägger ingen skyldighet att iaktta någon viss standard för riskhantering, utan beroende på televerksamhetens omfattning och karaktär kan förfaranden på olika nivåer tillämpas. Bland annat följande standarder och publikationer om riskhantering har getts ut: ISO/IEC 27005 och NIST 800-30 Risk Management Guide. Riskhanteringsmodeller skiljer sig i olika företag, och en enda modell som skulle passa för alla finns inte.

Föreskriften förutsätter att riskhanteringen är en kontinuerlig process. Enligt detta ska riskerna och metoderna för hantering av dem bedömas alltid när omständigheterna förändras, till exempel som en del av anskaffningen av och processen för ibruktagande av nya tjänster, i samband med förändringar (se förändringshantering i punkt 7.2) eller efter att en eventuell risk har realiserats.

För teleföretag i mobilnätet är det viktigt att beakta de interna och externa hot som riktar sig mot i synnerhet komponenter i 5G-näten och -tjänsterna och som delvis är nya. Föreskriften förutsätter att teleföretaget har en riskhanteringsprocess som syftar till att hantera och lindra riskerna som hoten orsakar mot bl.a. de aktuella egendomarna. Dessutom är det motiverat att ägna särskild uppmärksamhet åt bedömningen av riskerna som gäller t.ex. virtualiseringsmiljöer och Edge Computing-enheter.

Dokumentation av processen och resultaten

Enligt punkt 4.2 i föreskriften ska teleföretaget för att övervaka riskhanteringens kontinuitet och iakttagandet av kraven spara de dokumenterade resultaten av riskhanteringsprocessen i minst tre år eller räknat från de tre sista behandlingarna, beroende på vilken lagringstid som är längre. Om antalet behandlingsomgångar inte uppnås under tre års tid, ska dokumentationen alltså sparas längre än tre år och å andra sidan, om det under en treårsperiod finns fler än tre behandlingsomgångar, ska alla dessa dokument sparas.

[23] ENISA GL SO2, 5G Security Control Matrix: M07–M013, SO2-001, SO2-003–SO2-005 och ISO/IEC 27005:2018: 8 och 9.

Dokumentering av riskbedömningen och lagring av tidigare resultat ger värdefull information om hur man har förhållit sig till liknande risker under tidigare behandlingsomgångar. Resultatet av en riskbedömning kan vara exempelvis behandling av nya uppgifter om hot som dock inte leder till någon förändrad riskbedömning.

4.3 Roller och ansvar inom informationssäkerhet

Enligt punkt 4.1.3 i föreskriften ska teleföretaget fastställa korrekta informationssäkerhetsroller och ansvar i anknytning till dem i överensstämmelse med informationssäkerhetspolicyn och verksamhetsprinciperna som ska genomföras.

Tydligt definierade och dokumenterade roller och ansvar inom informationssäkerheten som hela personalen känner till möjliggör ett systematiskt genomförande av informationssäkerheten och en struktur för hanteringen av informationssäkerheten som stöder informationssäkerheten i det dagliga arbetet. Beroende på omfattningen av teleföretagets verksamhet och de olika informationssäkerhetsrollernas karaktär kan ansvaret vara en del av personalens övriga uppgiftsbeskrivning. Vid genomförandet av punkten kan man till tillämpliga delar stödja sig på åtgärderna och informationssäkerhetskontrollerna i enlighet med ENISAs riktlinjer.[24] I praktiken är det motiverat att tydligt precisera i synnerhet de skyldigheter som gäller ombesörjandet av informationssäkerheten för de viktigaste delarna i kommunikationsnätet och för andra betydande objekt som ska skyddas.

Dessutom ska teleföretaget i enlighet med föreskriften i den mån det är möjligt förhindra uppkomsten av ansvars- och uppgiftshelheter som äventyrar informationssäkerheten genom att separera sinsemellan motstridiga uppgifter och ansvarsområden, såsom till exempel begäran om, godkännande och beviljande av behörigheter.[25] Uppkomsten av sådana ansvars- och uppgiftshelheter kan tillfälligt tillåtas, om de risker som hänför sig till situationen har bedömts och lämpliga hanteringsåtgärder har vidtagits. Om det emellertid är till exempel fråga om en liten aktör är det inte nödvändigtvis möjligt att i praktiken separera alla motstridiga uppgifter i sin helhet. Då ska de risker som verksamheten medför hanteras på andra sätt, till exempel genom teknisk övervakning och loggning av åtgärderna.

Det är motiverat att dokumentera de delområden som en enskild person eller en nyckelperson ansvarar för och att behandla de identifierade riskerna i anknytning till situationen.

I punkt 5.1.2 i föreskriften föreskrivs om personalens kunskaper och utbildning i informationssäkerhet.

Det är bra att observera att de inbördes relationerna mellan informationssäkerhetsrollerna och ansvarspersonerna regelbundet ska granskas som en del av upprätthållandet av den informationssäkerhetspolicy och verksamhetsprinciper som förutsätts i punkt 4.1.1 i föreskriften. Vid genomförandet av detta är det bra att i praktiken beakta förändringar i verksamhetsmiljön, personalbyten och upptäckta avvikelser (se även punkterna 4.1.3, 5.1.3 och 5.1.4 i föreskriften).

4.4 Leverantörsrelationer

Hantering av leverantörsrelationerna är en viktig del av teleföretagens riskhantering. Exempelvis otillräcklig riskhantering i underleverantörskedjorna för centrala delar av

[24] ENISA GL SO3, 5G Security Control Matrix: M014–M018, SO3-001 och ISO/IEC 27002:2022: 8.8.
[25] Likaledes ISO/IEC 27002:2022: 5.3

kommunikationsnät eller andra funktioner som är viktiga med tanke på informationssäkerheten kan leda till att informationssäkerheten i hela kommunikationsnätet eller -tjänsten äventyras.

Punkt 4.1.4 i föreskriften förutsätter att teleföretaget utarbetar preciserande verksamhetsprinciper och riskhanteringsprocesser för att hantera riskerna i leveranskedjorna. Punkten motsvarar SO4 enligt ENISAs riktlinjer, och i genomförandet av den kan man till tillämpliga delar stödja sig på de åtgärder som ENISA fastställt och de informationssäkerhetskontroller som stöder dem.[26]

Kravet i föreskriften avser alltså i praktiken att teleföretaget ska tillämpa förfaranden genom vilka det säkerställer att tredje parter, till exempel utrustnings-, programvaru- och tjänsteleverantörer, samt samarbetspartner för samtrafik och övriga samarbetspartner följer den informationssäkerhetsnivå som teleföretaget förutsätter. I praktiken är det bra för teleföretaget att definiera lämpliga informationssäkerhetskrav för avtal med tredje parter. Genom kraven säkerställer man att teleföretagets informationssäkerhetspolicy eller andra anvisningar genomförs. Teleföretaget kan till exempel kräva att lämpliga säkerhetsstandarder iakttas i leverantörens produkter, tjänster och verksamhet.

I de verksamhetsprinciper som gäller leverantörsrelationer är det bra att specificera förfarandena för att ombesörja informationssäkerheten i leverantörsrelationerna, förfarandena relaterade till övervakning av leverantörerna samt hanteringen av eventuella kvarstående risker som genom leverantörens egna åtgärder inte nått en nivå som godkänns av teleföretaget.

Det är bra att verksamhetsprinciperna omfattar ett register som ska upprätthållas över avtal som ingåtts med leverantörer, med hjälp av vilket avtalen vid behov kan granskas regelbundet till exempel för att säkerställa att informationssäkerhetskraven är aktuella.

Teleföretaget bör fastställa lämpliga förfaranden för leverantörsrelationerna för ändamålsenligt skydd av de data som flyttas eller behandlas (se även punkt 6.1.4 i föreskriften) samt de skyldigheter som gäller uppgifternas sekretess.[27]

Det finns också skäl att följa upp hur kraven på informationssäkerhet uppfylls i tredje parters verksamhet. Detta kan göras exempelvis med hjälp av revisioner eller till exempel genom att kräva regelbunden, oberoende rapportering av leverantörens metoder för att hantera informationssäkerheten och deras effekt.

Det är bra att verksamhetsprinciperna också omfattar uppföljning av avvikelser som beror på tredje parters verksamhet och till exempel metoder för att säkerställa att de programkomponenter som tredje parter levererar är äkta och beständiga.[28]

Teleföretaget ska enligt punkt 4.1.1 i föreskriften regelbundet granska och uppdatera sina preciserande verksamhetsprinciper med beaktande av förändringarna i verksamhetsmiljön och de avvikelser som observerats i leverantörernas verksamhet.

[26] ENISA GL SO4, 5G Security Control Matrix: M019–M026, SO4-004–SO4-014 och SO4-016–SO4-048.
[27] ISO/IEC 27002:2022: 5.20.
[28] Om metoderna se t.ex. NIST, Defending Against Software Supply Chain Attacks (April 2021).

5. Personalsäkerhet

5.1 Personalens tillförlitlighet

Enligt punkt 5.1.1 i föreskriften ska teleföretag genomföra nödvändiga utredningar av sin personal för att säkerställa att den inom ramarna för tillämplig lagstiftning är tillförlitlig i de fall då det med avseende på en persons uppgift och ansvar är nödvändigt. Punktens motsvarighet är SO5 enligt ENISAs riktlinjer, och i genomförandet av den kan man stödja sig på till exempel de åtgärder som ENISA fastställt och de informationssäkerhetskontroller som stöder dem.[29] Teleföretaget ska i förväg fastställa verksamhetsprinciper och förfaranden för att genomföra bakgrundskontroller av personer, eftersom teleföretaget ska dokumentera på vilket sätt det tar kravet i beaktande samt upprätta en informationssäkerhetspolicy och närmare verksamhetsprinciper i anknytning till den (punkterna 3.2 och 4.1.1 i föreskriften).

I rekryteringen ska teleföretaget genomföra en lämplig bakgrundskontroll av utvalda personer om det anses nödvändigt med tanke på personernas arbetsuppgifter. I genomförandet av bakgrundskontroller ska tillämplig lagstiftning som gäller dataskydd samt säkerhetsutredningar och utredningar om tillförlitlighet inom arbetslivet, t.ex. säkerhetsutredningslagen (726/2014) och kreditupplysningslagen (527/2007), beaktas.

Bakgrundskontrollerna ska ställas i relation till de identifierade riskerna och klassificeringen av de data som behandlas. Processen för bakgrundskontroller ska tillämpas även på hyrda arbetstagare och utomstående leverantörer, när det är motiverat i förhållande till riskerna med användning av sådan personal. Om man med hjälp av metoderna inom processen för bakgrundskontroller inte uppnår en godtagbar risknivå bör teleföretaget ha förfaranden för hantering av de kvarstående riskerna. Om de kvarstående riskerna inte kan minskas till en godtagbar nivå ska personen inte tilldelas uppgiften i fråga. De kvarstående riskerna kan hanteras exempelvis med metoder för åtkomstkontroll eller genom att genomföra separat övervakning.

Vid genomförande av bakgrundskontroller och fastställande av kontrollernas omfattning bör man särskilt beakta de roller där personerna har fysisk eller logisk tillgång till de kritiska delarna av mobilnätet eller ett annat centralt kommunikationsnät eller till andra betydande objekt som ska skyddas.

Förpliktelsen anknyter även till skyldigheten enligt punkt 5.1.3 i föreskriften att kunna hantera risker som förändringar inom personalen eller personalens uppgifter medför. När en person övergår till en sådan roll inom teleföretaget ska teleföretaget bedöma huruvida den tidigare bakgrundskontrollen är tillräcklig och vid behov göra en bakgrundskontroll som motsvarar rollen. Det skulle också i övrigt vara bra att vid behov upprepa bakgrundskontrollerna regelbundet, vid behov med beaktande av säkerhetsutredningarnas giltighetstider.

Teleföretaget ska vid behov granska och uppdatera de riktade verksamhetsprinciper och förfaranden som utarbetats för genomförandet av bakgrundskontroller med beaktande av förändringarna i verksamhetsmiljön och hoten samt de observerade säkerhetsavvikelserna, såsom punkt 3.1 i föreskriften förutsätter i praktiken.

[29] ENISA GL SO5 samt 5G Security Control Matrix: M027–M030 och SO5-001. Se även ISO/IEC 27002:2022: 6.1.

5.2 Personalens kunskaper i informationssäkerhet och utveckling av den

Enligt punkt 5.1.2 i föreskriften ska teleföretag ha förfaranden för att säkerställa och upprätthålla tillräcklig informationssäkerhetskompetens för personalen. Teleföretag ska ordna utbildning i informationssäkerhet för personalen som enligt behov kan vara allmän eller uppgiftsinriktad. Det är motiverat att följa upp deltagandet i utbildningarna. I allmänna informationssäkerhetsutbildningar bör man beakta till exempel förebyggande av spridning av skadliga program samt i synnerhet sträva efter att utveckla och upprätthålla personalens medvetenhet och beredskap att agera för att avvärja nätfiske.[30]

Teleföretag ska göra personalen medveten om informationssäkerhetspolicyn och de riktade verksamhetsprinciperna, målen för dessa och konsekvenserna vad beträffar personalens egna arbetsuppgifter.[31]

Det är bra att i praktiken regelbundet se över och uppdatera innehållet i informationssäkerhetsutbildningarna med beaktande av förändringar i verksamhetsmiljön, resultaten av utvärderingar och observerade avvikelser.

För att verifiera personalens kunskaper i informationssäkerhet kan teleföretaget införa förfaranden för att testa nivån på personalens kunskaper. Dessutom kan teleföretaget ta i bruk metoder med vilka dess personal, till exempel anonymt, kan anmäla de upptäckta informationssäkerhetshoten, informationssäkerhetskränkningarna, informationssäkerhetsriskerna eller utvecklingsobjekten. Med dessa åtgärder kan teleföretaget bygga upp sin egen informationssäkerhetskultur.

5.3 Upphörande av och förändringar i anställningsförhållanden

Enligt punkt 5.1.3 i föreskriften ska teleföretaget ha dokumenterade förfaringssätt för att kunna hantera informationssäkerhetsrisker som personalförändringar eller förändringar i personalens uppgifter medför.[32]

Till förfaringssätten hör i praktiken att teleföretaget gör sin personal förtrogen med arbetsuppgifterna och de förändringar som sker i dem, samt att teleföretaget vid behov utan dröjsmål tar ur bruk onödiga behörigheter, passerkort, identitetskort och utrustning när det sker förändringar inom personalen och i uppgifterna.

Punkt 5.1.2 i föreskriften föreskriver om personalens kunskaper i informationssäkerhet och att personalen känner till verksamhetsprinciperna relaterade till i synnerhet de egna arbetsuppgifterna.

Enligt punkt 3.2 i föreskriften ska teleföretaget i praktiken se till att de verksamhetsprinciper och förfaringssätt som anknyter till förändringar i personalen eller personalens uppgifter är aktuella genom att beakta förändringar i verksamhetsmiljön och observerade avvikelser.

5.4 Åtgärder av personalen som strider mot informationssäkerhetspolicyn

Teleföretaget ska ha ett dokumenterat förfarande för hur man ingriper i situationer där en arbetstagare bryter mot teleföretagets verksamhetsprinciper eller förfaranden som gäller informationssäkerheten. I praktiken ska förfarandet omfatta till exempel hur man

[30] ENISA GL SO6 och ISO/IEC 27002:2022: 6.2, 6.3, 6.6 och 8.7. Se även https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/rad-identifiering-av-tvivelaktiga-sidor.
[31] 5G Security Control Matrix: M004 och ISO/IEC 27002:2022: 5.1.
[32] ENISA GL SO7 och ISO/IEC 27002:2022: 6.2, 6.5, 6.6.

behandlar situationer där en informationssäkerhetskränkning beror på personalens verksamhet som strider mot informationssäkerhetsprinciperna.[33] Det är också bra att som en del av förfarandet bedöma med vilka eventuella åtgärder avvikelserna kan undvikas i fortsättningen.

En informationssäkerhetskränkning eller ett hot mot den ska anmälas till tillsynsmyndigheten samt till abonnenter och användare i enlighet med tillämplig lagstiftning.

6. Säkerhet inom informationssystem och telekommunikationsområdet samt fysisk säkerhet

6.1 Åtkomsthantering

För åtkomsten till teleföretagets kommunikationsnät och informationssystem ska det finnas ändamålsenliga logiska, fysiska och administrativa mekanismer för åtkomsthantering, vilka omsorgsfullt upprätthålls under hela användaridentitetens livscykel.[34]

Föreskriften förutsätter att teleföretaget definierar och dokumenterar riktade verksamhetsprinciper och förfaranden som beaktar kraven för informationssäkerhet inom åtkomsthanteringen och genom vilka man säkerställer endast lovlig åtkomst till komponenterna i kommunikationsnätet eller -tjänsten samt de uppgifter som behandlas i samband med televerksamheten. Kraven för åtkomsthanteringen ska även kommuniceras till de intressenter som genom teleföretagets auktorisering deltar i hanteringen av behörigheter.

I praktiken beskriver man i verksamhetsprinciperna åtminstone reglerna för åtkomsthanteringen och identitetshanteringen samt principerna för beviljande och hantering av åtkomsträttigheter och behörigheter.

Reglerna för åtkomsthanteringen genomförs genom att definiera åtkomsträttigheter och åtkomstbegränsningar i enlighet med kraven. Behörighet kan beviljas en person eller ett tekniskt eller logiskt objekt, till exempel en maskin, en anordning eller en tjänst. Utgångspunkten för åtkomsthanteringen bör alltid vara principen om lägsta behörighet. Det är dessutom bra att beakta åtskiljandet av uppgifter i samband med ansökan om och beviljande av behörigheter (se även punkt 4.1.3 i föreskriften).[35]

Det finns flera olika sätt att genomföra hantering av behörigheter, på vilka hanteringen även kan automatiseras och underlättas. Inom rollbaserad åtkomsthantering baserar sig behörigheterna på användarnas roller, varvid det är särskilt viktigt att sinsemellan motstridiga informationssäkerhetsroller och -ansvar har åtskilts i enlighet med den tredje strecksatsen i punkt 4.1 i föreskriften. Med hjälp av exempelvis dynamisk åtkomsthantering kan man dessutom begränsa tillträdet tidsmässigt eller till endast en viss del av informationen samt skydda komponenter i kommunikationsnätet och -tjänsterna som är kritiska med tanke på driftskontinuiteten.

Genom en identifierad identitet gör man det möjligt att individuellt identifiera och hantera användare. Inom identitetshanteringen strävar man efter att utgångspunkten är användning av personliga identiteter. Om detta i ett enskilt system inte är tekniskt möj-

[33] ENISA GL SO7 och ISO/IEC 27002:2022: 6.2, 6.4, 6.5, 6.6.
[34] ENISA GL SO11.
[35] ISO/IEC 27002:2022: 5.15, 5.16, 8.2.

ligt eller kostnadsmässigt rimligt är det bra att förfaringssätten för att identifiera användarna genomförs och dokumenteras i praktiken på ett tillräckligt sätt med hjälp av metoder utanför systemet (t.ex. med hjälp av en s.k. hoppmaskin).

Verksamhetsprinciperna ska dokumenteras enligt punkt 3.2 i föreskriften.

Krav som gäller personalförändringar behandlas även i kapitel 5.3 i motiveringspromemorian.

6.2 Skydd av nätens och informationssystemens integritet

Föreskriften förutsätter att teleföretaget sköter om integriteten hos sina nät och tjänster samt terminalerna och informationssystemen som personalen använder och skyddar dessa mot virus, tillägg av skadlig kod och skadlig programvara som skulle kunna ändra funktionerna i systemen.[36] De verksamhetsprinciper som förutsätts enligt denna skyldighet ska dokumenteras i enlighet med punkt 3.2 i föreskriften.

Skydd, förvaltning och övervakning av nät och tjänster samt av den utrustning som förverkligar dem är viktiga för att skydda data i system och applikationer från att bli äventyrade via nätet. För att genomföra detta bör teleföretaget ha i bruk kontroller för att kunna säkerställa informationssäkerheten i nätet och skydda tjänster som anslutits till nätet från olovlig användning.

Det är viktigt att den terminalutrustning som teleföretagets personal använder i sitt arbete administreras, används och skyddas på korrekt sätt, eftersom terminalutrustning som används på bristfälligt sätt eller i strid med anvisningarna kan utsättas för skadliga program och nätfiske, och på så sätt fungera som ingångar till teleföretagets nät eller data.[37]

I praktiken är det bra för teleföretaget att ha riktade verksamhetsprinciper och standardförfaranden som i enlighet med informationssäkerhetspolicyn fastställer metoder för att i miljöer med olika klassificeringsnivå hantera informationssäkerheten för terminalutrustning samt beskriva personalens ansvar för att genomföra hanteringsmetoderna. Krav gällande personalens utbildning behandlas i punkt 5.1.2 i föreskriften.

Det är möjligt att skydda sig mot skadliga program exempelvis genom att begränsa behörigheterna enligt principerna om lägsta behörighet eller härda systemen, genom lämpliga installationsrutiner för säkerhetsuppdateringar, utbildningar i medvetenhet om informationssäkerhet för personalen samt med hjälp av program för upptäckt och korrigering av skadliga program.[38]

Hanteringen av sårbarheter stöds av en tillräckligt exakt och omfattande hantering av egendom som om det är möjligt baserar sig på automation och som innehåller nödvändig information om beroendeförhållandena mellan olika program (hierarki, system), information om leverantören av programmet, programmets namn och version samt uppgifter om de personer som ansvarar för programmet.[39] I punkt 7.1.3 föreskrivs om tillvägagångssätt för att hantera egendom.

Säkerhetsåtgärder för komponenter i mobilnät behandlas även i punkt 10 i föreskriften.

[36] ENISA GL SO12.
[37] ISO/IEC 27002:2022: 8.1
[38] ISO/IEC 27002:2022: 8.7
[39] ISO/IEC 27002:2022: 8.8.

Principen om nolltillit (zero trust) är en informationssäkerhetsmodell som begränsar åtkomsten för system och användare till endast nödvändiga resurser samt som minimerar riskerna till följd av olovlig åtkomst.[40] Inom modellen är även upprepad autentisering och auktorisering mellan entiteter ett tvång. Inom modellen antas att en angripare alltid är närvarande, vilket innebär att utgångspunkten är att ingen komponent och inget system är pålitligt. Det är motiverat att tillämpa denna informationssäkerhetsmodell på teleföretagets trafik som sker i nätet i synnerhet när det är fråga om komponenter som är centrala med tanke på kontinuiteten och modellen är tekniskt lämplig.

Utvidgning av ett intrång (lateral movement) är ett begrepp som avser en angripares rörelse inne i det nätverk som är föremål för angreppet efter att denne fått fotfäste i något av nätverkets system. Denna begränsning av rörelse kan göras exempelvis genom att dela in nätet i domäner enligt tillitsnivå.[41]

Det är bra att utarbeta egna riktade verksamhetsprinciper och standardförfaranden för att dela in näten i olika domäner, zoner eller segment enligt olika tillitsnivåer samt skilja domänerna från varandra antingen fysiskt eller logiskt (t.ex. med hjälp av virtuella separata nät). Det är bra att åtskilja domänerna från det offentliga nätet alltid när det är möjligt. Ett av syftena med åtskiljandet är att göra det svårare för angriparen att röra sig i nätet mellan olika domäner om angriparen lyckas få fotfäste inne i en domän. Även principen om nolltillit som beskrivs ovan stöder denna tanke. Det är bra att kriterierna, med hjälp av vilka näten delas in i olika domäner, i praktiken baserar sig på en bedömning av säkerhetskraven för respektive domän. Åtskiljandet kan göras exempelvis så att man försöker skilja de nätskikt som transporterar användar-, styr- och kontrolltrafiken från varandra med hjälp av ovanstående metoder. Trafik och åtkomst mellan domänerna kan tillåtas, men i sådana fall bör man se till att det finns övervakning mellan domänerna och möjlighet att begränsa trafiken så att endast trafik som är nödvändig och oundviklig för verksamheten tillåts. Trafiken kan filtreras och övervakas med hjälp av exempelvis brandväggar, routrar, nätslussar för applikationsskiktet eller separata system för förhindrande av intrång (IPS) och för detektering av intrång (IDS).[42]

I verksamhetsprinciperna bör man tänka på att i den mån det är möjligt ta tjänster och protokoll som är onödiga med tanke på nätets logiska och fysiska gränssnitt och anslutningar ur bruk. Logiska och fysiska gränssnitt är nätslussar med hjälp av vilka nätutrustningen kommunicerar med externa utrustningar och system. De tjänster och protokoll som tillhandahålls i gränssnitt möjliggör olika slags funktionalitet, och ju fler sådana protokoll och tjänster som används samtidigt, desto större är risken för att de utnyttjas även vid eventuella angrepp.

6.3 Skydd mot överbelastningsangrepp

Enligt punkt 6.3 i föreskriften ska teleföretaget skydda de system som är centrala med tanke på kommunikationsnäten och -tjänsterna mot överbelastningsangrepp. Skyddsåtgärderna ska dimensioneras i enlighet med en aktuell riskbedömning. Riskbedömningen ska alltså basera sig på aktuell information om hot. Upprätthållandet av medvetenheten om hot kan omfatta exempelvis informationsutbyte med olika samarbetsnätverk och aktuell uppföljning av olika källor med hjälp av lämpliga verktyg. Medvetenheten om hot behandlas i punkt 9 i föreskriften.

[40] NIST - Zero Trust Architecture - SP.800-207, https://csrc.nist.gov/publications/detail/sp/800-207/final.
[41] Informationssäkerhet nu! Känner du till lateralt intrång (del 1 och 2), https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/kanner-du-till-lateralt-intrang-del-1 och https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/kanner-du-till-lateralt-intrang-del-2.
[42] ISO/IEC 27002:2022: 8.22.

Överbelastningsangrepp (Denial of Service attack) är ett angrepp som syftar till att förhindra användning av en nätresurs eller en tjänst i ett nät. Överbelastningsangrepp utförs vanligtvis genom att belasta den tjänst/nättrafik som är målet med extra trafik eller genom att utnyttja en sårbarhet i objektet. Numera är en stor del av överbelastningsangreppen spridda, vilket betyder att angreppet kommer från flera enheter samtidigt. På så vis möjliggör man exempelvis användning av en större trafikmängd för att överbelasta den angripna tjänsten. Bakgrunden till spridda angrepp är ofta enheter som har kapats för att användas vid angrepp utan att ägarna vet om det.

Sätten att genomföra överbelastningsangrepp varierar. Vid ett angrepp belastas oftast ett objekt med en stor mängd trafik, varvid den angripna nätresursens eller tjänstens nivå sjunker eller blockeras. Ett exempel på en allmänt använd typ av överlastningsangrepp är ett så kallat SYN-översvämningsangrepp (SYN flood), som baserar sig på en trevägshandskakning via TCP-protokollet. I angreppet skickar angriparen en stor mängd TCP SYN-paket till objektet, men inga ACK-paket alls, vilket innebär att den angripna servern eller enheten fylls av halvfärdiga förbindelser och inte kan ta emot nya kontaktförfrågningar.

Ett överbelastningsangrepp kan även göras på applikationsnivå. I sådana fall riktar angriparen sitt angrepp mot applikationen i sig genom att utnyttja sårbarheter eller allmänt kända problem. Sådana angrepp kräver nödvändigtvis inga stora mängder trafik för att fungera och är därför svårare att upptäcka. Ett exempel på ett sådant angrepp är HTTP-översvämningsangrepp (HTTP flood), där angriparen skickar en behövlig mängd HTTP-förfrågningar till ett utvalt objekt så att andra användare inte kan använda objektet. Dessa HTTP-förfrågningar kan vara svåra att skilja från förfrågningar från riktiga människor, och därför kan det vara utmanande att upptäcka den här typen av angrepp.

I och med nya teknologier och tekniker är även föremålen för, mängden och kvaliteten på överbelastningsangreppen i ständig förändring. Exempelvis angrepp mot olika gränssnitt i 5G-nät skapar nya utmaningar för tjänsteleverantörerna. 5G-nät möjliggör mångfaldig enhetstäthet jämfört med tidigare nätgenerationer, och exempelvis mängden IoT-enheter (Internet of Things, IoT) som används för potentiella överbelastningsangrepp väntas öka. Ökningen av mängden enheter och en eventuell varierande nivå på informationssäkerheten förutsätter att man beaktar riskerna och förbereder sig för dem.

Typiska sätt att lindra effekterna av överbelastningsangrepp är exempelvis paketfilter, som sprider nättrafiken, eller genom att använda SAV-tekniker (Source Address Validation), till exempel ACL (Access Control Lists), där man bland annat kan definiera vilka IP-prefix som ska förkastas i nättrafiken.[43] Konsekvenserna av överbelastningsangrepp kan minskas även med hjälp av korrekta konfigurationer av utrustning såsom brandväggar och lastbalanserare. IDS- (Intrusion Detection System) och IPS-system (Intrusion Prevention System) som antingen fungerar separat eller ingår i brandväggen hjälper till att upptäcka och förhindra överbelastningsangrepp.

6.4 Användning av kryptering och kryptografi

Genom att använda kryptografi skyddas konfidentialiteten, äktheten och integriteten hos data. Med hjälp av ändamålsenlig kryptering förhindras och minimeras konsekvenserna av informationssäkerhetsstörningar för användarna, nätverken och tjänsterna. Skyldigheterna i föreskriften som gäller kryptering motsvarar delvis de skyldigheter som föreskrivs i svenska Post- och telestyrelsens (PTS) föreskrift och dess tillämpningsanvisningar.[44]

[43] NIST – Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation, s. 27–28, https://csrc.nist.gov/publications/detail/sp/800-189/final.
[44] Post- och telestyrelsens föreskrifter och allmänna råd om säkerhet i nät och tjänster, PTSFS 2022:11, 10 kap, https://www.pts.se/sv/dokument/foreskrifter/telefoni--internet/ptsfs-202211---foreskrifter-och-allmanna-rad-om-sakerhet-i-nat-och-tjanster/.

Enligt föreskriften ska teleföretaget utarbeta och upprätthålla förfaranden i enlighet med de riktade verksamhetsprinciper (krypteringspolicy) som gäller kryptering. Verksamhetsprinciperna ska innehålla information om åtminstone sätten att genomföra krypteringen samt om när och i vilka situationer som kryptering eventuellt inte används. Verksamhetsprinciperna ska även innehålla allmän information om funktionen och styrkan hos krypteringsmetoderna samt vilken typ av metod som används. Verksamhetsprinciperna ska dessutom innehålla beskrivningar av vilken skyddsnivå som data kräver samt av vilken krypteringsmetod som lämpar sig för kryptering av vilka data.[45]

Olika typer av information är förknippade med olika risker som varierar beroende på hotnivån i miljön. Teleföretaget bör alltid från fall till fall bedöma det behov av kryptering och den krypteringsnivå som data kräver samt de krypteringsmetoder som är ändamålsenliga. I synnerhet lösenord, krypteringsnyckelmaterial och andra hemliga uppgifter som används vid autentisering ska alltid krypteras om det är tekniskt möjligt. För krypteringen bör alltid krypteringslösningar och krypteringsprotokoll som lämpar sig för situationen och som ger ett tillräckligt skydd användas. Vid bedömningen av krypteringsbehovet kan man till exempel beakta om det är tillräckligt att någon del av trafiken är krypterad i vissa situationer. Det är till exempel möjligt att man genom att kryptera styrtrafiken uppnår en tillräcklig nivå av informationssäkerhet, varvid det inte finns något separat behov av att kryptera trafik på användarnivå. Dessutom kan man i riskbedömningen beakta de olika informationssäkerhetsriskerna som orsakas av överföringssättet för trafiken. Bedömningen påverkas också av sådana omständigheter som olika aktörers möjligheter att få åtkomst till trafiken och om trafiken till exempel går över internet, i betrodda partners nät eller enbart i teleföretagets eget nät, samt teleföretagets förmåga och behov att upptäcka skadlig trafik.

Enligt föreskriften ska ändamålsenlig kryptering användas alltid när data lagras eller överförs, om den med tanke på datas karaktär är ändamålsenlig, tekniskt möjlig och proportionerlig. Om data krypteras när den överförs eller lagras är det skäl att välja en teknik som ger tillräckligt skydd med tanke på klassificeringen av de data som ska krypteras och prestandakraven. När det gäller krypteringstekniken är det bra att beakta algoritmer, användningssätt och nyckelstyrkor. Kraven på den krypteringsmetod som används bör vara aktuella under systemets hela livscykel. Om kryptering inte är möjlig ska teleföretaget motivera det i sina verksamhetsprinciper som det upprätthåller. Om kryptering inte används vid lagring eller överföring av data ska teleföretaget i praktiken utarbeta en risk- och konsekvensbedömning om saken i fråga som en del av genomförandet av kravet i punkt 4.1.2 i föreskriften, och beskriva den i verksamhetsprinciperna.[46]

Det kan vara utmanande att ersätta brister i krypteringsmetoderna med andra skyddsmetoder, vilket innebär att teleföretaget ska ägna uppmärksamhet åt valet av krypteringslösningar och säker användning.[47] Särskild uppmärksamhet ska ägnas åt valet och användningen av de krypteringsprotokoll som används för att skydda komponenter som är centrala med tanke på kommunikationsnätets eller -tjänstens driftskontinuitet samt åt skyddet av komponenter som innehåller eller behandlar känsligt datamaterial.

[45] ENISA GL SO13, 5G Security Control Matrix: M071, M073 och M074.
[46] ENISA GL SO13, 5G Security Control Matrix: M072.
[47] På motsvarande sätt åt Katakri 2020 – kvalitetsrevision för informationssäkerhet för myndigheter (Katakri 2020 - tietoturvallisuuden auditointityökalu viranomaiselle). I-12, s. 89, https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille.

Exempelvis för att kryptera datatrafik bör man i fråga om TLS-krypteringsprotokollet använda minst version 1.2 eller senare. Versionerna 1.0 och 1.1 av TLS-protokollet är föråldrade och ska inte längre användas.[48]

6.5 Skydd och hantering av krypteringsnyckelmaterial och hemliga uppgifter som används vid autentisering

Punkt 6.1.5 i föreskriften förutsätter att teleföretag ska ha ändamålsenliga verksamhetsprinciper och förfaringssätt för att skydda och behandla hemliga uppgifter i krypteringsnyckelmaterialen och hemliga uppgifter som används vid autentisering. Detta är viktigt, eftersom om dessa hamnar i fel händer skulle det bland annat äventyra telekommunikationssäkerheten och effektiviteten i hanteringsförfarandena för åtkomst.

Teleföretaget ska alltså i praktiken försäkra sig om att krypteringens nyckelmaterial eller hemliga autentiseringsuppgifter, inklusive krypteringsnyckelmaterial som används vid autentisering, inte röjs och att de skyddas från ändring och försvinnande. Krypteringsnycklarna ska alltså endast användas av de användare och processer som är avsedda för dem. Det är bra att skydda krypteringsnyckelmaterial och hemliga autentiseringsuppgifter samt utrustning som används för att skapa, lagra och arkivera krypteringsnycklar med hjälp av bästa praxis och standarder för informationssäkerhet.[49] Vid skyddet av krypteringsnyckelmaterial och andra hemliga uppgifter som används för autentisering är det motiverat att använda även kryptering.

Verksamhetsprinciperna och förfarandena för hantering av krypteringsnycklar ska vara planerade, genomförda och beskrivna. Teleföretaget ska alltså i praktiken ha rutiner beträffande användningen och skyddet av samt livslängden på krypteringsnycklarna. I verksamhetsprinciperna är det skäl att även definiera rollerna och ansvaren samt övervakningen under krypteringsnycklarnas hela livslängd, inklusive användning, säkerhetskopiering och återställande av privata nycklar.[50]

6.6 Härdning av virtualiseringsmiljöer

I punkt 6.1.6 i föreskriften förutsätts att komponenterna i kommunikationsnät och -tjänster som genomförts i en virtualiseringsmiljö genomförs så att man endast tillåter funktioner och behörigheter som är nödvändiga för att komponenterna ska fungera. Med andra ord förutsätter föreskriften en så kallad härdning av virtualiseringsmiljöerna. Teleföretaget ska ha dokumenterade verksamhetsprinciper och förfaranden för härdning av virtualiseringsmiljöer (punkt 3.2 i föreskriften).

Med *virtualisering* avses en process där man simulerar en funktionalitet genom att skapa en virtuell beräkningsmiljö för den, med hjälp av vilken funktionaliteten skiljs från den fysiska resursen i bakgrunden.[51] En *virtualiseringsmiljö* består av flera komponenter och

[48] IETF RFC 8996, Deprecating TLS 1.0 and TLS 1.1, https://www.rfc-editor.org/rfc/rfc8996.
[49] ENISA GL SO14, 5G Security Control Matrix: M075.
[50] ENISA GL SO14, 5G Security Control Matrix: M076 och M077.
[51] Virtualisering avlägsnar en fysisk resurs från andra system, applikationer och användare. Inom virtualisering kan samma fysiska resurs som finns i bakgrunden, t.ex. en server, ett minne eller en processor, fungera som flera logiska resurser eller, om det finns flera fysiska resurser, kan de med hjälp av virtualisering framställas som en logisk helhet. Virtualisering kan tillämpas på flera olika delområden, t.ex. servrar, datakraft, nätverk, lagringsutrymme, operativsystem och applikationer. Virtualisering kan göras på olika sätt. Det första sättet är att skapa en virtuell maskin, som programmässigt har skapats för att emulera ett främmande operativsystem. För en fysisk utrustning kan man skapa flera virtuella maskiner, som använder värdutrustningens resurser för att köra program och funktioner. Beträffande virtuella maskiner skapar och kör en virtualiseringsplattform (hypervisor) de virtuella maskinerna. Virtualiseringsplattformen ansvarar för fördelningen av värdutrustningens resurser mellan de virtuella maskinerna. Ett annat sätt att genomföra virtualisering är med

system. Inom virtualiseringsarkitekturen pratar man i regel om följande komponenter och system: fysisk utrustning, virtualiseringsnivå, virtualiseringens hanteringsnivå, enskilda virtualiserade system samt operativa stödsystem och stödsystem för televerksamhet. Ju fler komponenter och olika leverantörer som används som stöd för virtualiseringen, desto mer sannolikt är det att det i virtualiseringsmiljön finns sårbarheter som hotar informationssäkerheten samt funktionalitet som är överflödig med tanke på den väsentliga användningen av systemet och som även kan visa sig vara en informationssäkerhetsrisk. Flera olika leverantörer medför utmaningar för hanteringen och uppföljningen av sårbarheter, vilket innebär att det är särskilt viktigt att obehövliga egenskaper tas ur bruk.

Med *härdning* avses återigen i detta fall att kommunikationsnätens och -tjänsternas komponenter installeras och upprätthålls så att endast *funktioner och behörigheter som är nödvändiga* för deras funktion används i dem. Genom att begränsa funktionerna, till exempel genom att ta bort onödiga applikationer och tjänster, minskas systemens sårbarhetsyta.

Teleföretaget kan själv bestämma på vilket sätt och med vilka tekniker det uppfyller kraven i föreskriften. Nedan presenteras de faktorer som det är bra för teleföretaget att beakta när det väljer ett genomförande som lämpar sig för sin egen verksamhet:

- I allmänhet är det bra att använda lämpliga verktyg i anslutning konfigurationshanteringen för att genomföra och upprätthålla en härdad installation.

- Begränsning av behörigheter är ett av sätten att genomföra en härdning. Här är det bra att följa principen om lägsta behörighet, det vill säga att behörigheter endast ges i enlighet med vad som är absolut nödvändigt. Det är även skäl att begränsa antalet sådana användare som har systemadministrativa behörigheter. Utöver de ovan nämnda är det ofta rimligt att begränsa åtkomsten och redigeringsrättigheter till känsliga filer, till exempel olika konfigurationsfiler.

- Det är skäl att hålla komponenter och system som väsentligen anknyter till produktionen och genomförandet av virtualiseringsmiljön, till exempel virtualiseringsplattformar och värdoperativsystem, aktuella med hjälp av regelbundna uppdateringar och skyddskorrigeringar. För detta kan man till exempel skanna program som väsentligen anknyter till produktionen och genomförandet av virtualiseringsmiljön regelbundet, så att det är möjligt att upptäcka sårbarheter i dem. Uppdateringarna kan skötas med regelbundna uppdateringspraxis, till exempel med månatliga korrigerings-/uppdateringsdagar. Dessutom är det bra om teleföretaget har egna processer för situationer där det uppstår kritiska sårbarheter i systemen. När det gäller sådana sårbarheter är det skäl att försöka göra uppdateringarna eller korrigeringarna så snart som möjligt.

- I praktiken är det bra att virtualiserade funktioner och komponenter i nätverket klassificeras och åtskiljs i administrativa domäner enligt komponentens eller funktionens riskfaktor. Det är även bra att i den mån det är möjligt sträva efter att skilja de administrativa domänerna från varandra eller åtminstone se till att trafiken mellan dem kan kontrolleras. Detta kan förverkligas genom att till exempel fördela arbetsbördan mellan olika segment utifrån deras informationssäkerhetsbehov och risk-

hjälp av containerisering (containerization). Containrarna skiljer sig från virtuella maskiner i det att de virtuella maskinerna virtualiserar ett helt operativsystem, medan containrarna virtualiserar endast de program och beroenden som containern behöver. Skapande och körning av containrar görs med hjälp av program som är avsedda för det.

klassificering samt genom att ansluta dessa segment till olika administrativa domäner. Risken kan bedömas enligt värdens typ, egenskaper och roll. Det är även skäl att observera att i en del kritiska system kan fysiskt åtskiljande vara nödvändigt.[52]

- Det är skäl att i den mån det är möjligt skilja hanteringsskiktet av virtuella miljöer från områden för förvaltning av sämre tillit, såsom operativ infrastruktur, teleföretagets eget interna nät, internet samt användarnät och andra nätverk inom teleföretagen. Åtskiljandet kan göras antingen fysiskt eller logiskt. Fysiskt åtskiljande kan göras till exempel så att funktioner i hanteringsskiktet inte körs på samma fysiska plattformar som funktioner i andra skikt. Logiskt åtskiljande kan återigen genomföras genom att till exempel använda separata virtuella maskiner för kontrollkomponenterna och funktionerna eller åtskilja nätskiktet med hjälp av vxlan, vlan eller kryptering av trafiken.

- Det är bra att skydda åtkomsten till hanteringsskiktet till exempel genom att använda multifaktorsautentisering, som genomförs genom att skapa en annan autentiseringsfaktor till exempel lokalt. Man kan också ställa in en tidsgräns eller en tidsutlösning för administrativ åtkomst. Det är motiverat att de koder som används för förvaltningen är personliga. Utöver personliga koder kan man även använda koder avsedda för nöd- eller undantagssituationer, då användningen av de personliga koderna är förhindrad. Det är skäl att begränsa användningen av dessa koder till endast på förhand dokumenterade användningsfall. Dessutom ska användningen av koderna kontrolleras tillräckligt väl med hjälp av metoder utanför målsystemet, med beaktande av de risker som är förknippade med detta.

- Beträffande tredje parter är det rimligt att bedöma behovet av hanteringsförbindelser från fall till fall samt iaktta principen om lägsta behörighet vid beviljande av behörigheter. I synnerhet när åtkomst till system och delar av sådana beviljas med hjälp av fjärråtkomst ska man se till att förbindelserna och de genomförda åtgärderna loggas på lämpligt sätt och dessutom överväga även andra revisionsåtgärder, genom vilka man säkerställer att inga otillåtna ändringar görs i nätverks- eller informationssystemen.

- Om containerteknik används i virtualiseringsmiljön och genomförandet av nätets funktioner är det viktigt i fråga om dessa se till att tillräckliga informationssäkerhetskontroller införs. Åtskiljandet av containrar från varandra kan uppnås exempelvis när containrar genomförs som processer under körning inne i definierade namnrymder (namespaces). Tilläggskontroller kan vara att till exempel begränsa körningen av containrarna med privilegier till minimum och säkerställa att höjning av rättigheterna inte tillåts. För containrar som körs med privilegier nedärvs rättigheterna vanligtvis från värddatorn, varvid omfattande rättigheter kan möjliggöra åtkomst till känslig information. De kan dessutom möjliggöra sådana skadliga API-anrop som kan göra det möjligt för en angripare att röra sig inuti kluster, det vill säga utvidga sitt intrång (lateral movement).

- I virtualiserade miljöer bör containrar och andra komponenter ha individuella identifierare som bidrar till att upptäcka och förhindra att eventuell intrång utvidgas.[53] Med hjälp av olika policyer och gruppdefinitioner kan man dessutom begränsa vilka resurser containrarna ser och hur mycket resurser (CPU, minne, lagringsutrymme,

[52] ENISA 5G Security Matrix: SO12-018 och ENISA NFV security in 5G: BP-T16, https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices.
[53] NSA – Security Guidance for 5G Cloud Infrastructures – Part I: Prevent and Detect Lateral Movement, s. 8, https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_I_508_Compliant.pdf.

nätverk) de tillåts använda samt hur det är möjligt att koppla nya kataloger till containrarna. Det är även motiverat att begränsa utförandet av processer inuti containrar med root-rättigheter. Bästa praxis och de bästa metoderna för informationssäkerhetskontroller inom de vanligaste containerteknikerna, t.ex. Kubernetes och Docker, finns exempelvis i de säkerhetshandböcker som organisationen Open Web Application Security Project (OWASP) utarbetat. OWASP är en organisation som fokuserar på att förbättra programvarusäkerheten.[54]

6.7 Fysisk säkerhet

I punkt 6.2 i föreskriften åläggs teleföretaget en skyldighet att utarbeta ändamålsenliga verksamhetsprinciper och förfaranden för att sörja för den fysiska säkerheten i informationssystemen, utrustningen, datamaterialen och lokalerna. Teleföretaget ska också ta hand om utrustningens miljöförhållanden. Teleföretaget ska alltså se till att på lämpligt sätt skydda de datamaterial, den utrustning samt de utrustningsutrymmen och andra utrymmen som används i televerksamheten mot fysiska hot. De hot som man ska skydda sig mot hänför sig i synnerhet till obehörig åtkomst samt till miljöfaktorer, såsom eldsvådor eller vattenskador.[55]

I Transport- och kommunikationsverkets föreskrift om säkerställande av kommunikationsnät och kommunikationstjänster samt om synkronisering av kommunikationsnät föreskrivs bl.a. om fysiskt skydd av utrustningsutrymmen och dokumentering av skyddet (punkt 17 i föreskriften). Föreskriften i fråga är dock inte en täckande föreskrift om fysisk säkerhet, och därför behandlas de aspekter som gäller den fysiska säkerheten till behövliga delar också i denna föreskrift om informationssäkerheten inom televerksamheten. Skyldigheten enligt punkt 6.2 i föreskriften gäller även de fall där ovanstående föreskrift om säkerställande av kommunikationsnät och kommunikationstjänster samt om synkronisering av kommunikationsnät inte ställer några särskilda krav på passerkontroll eller andra krav och omfattar förutom utrustningsutrymmen även lokaler som används för arbete.[56]

I verksamhetsprinciperna och förfarandena ska man vid behov beakta hur viktigt objektet som ska skyddas är, till exempel huruvida det är fråga om en kritisk del av kommunikationsnätet. Andra faktorer som ska beaktas även i riskbedömningen är t.ex. lokalernas läge och omgivningens säkerhet. Beträffande utarbetandet av verksamhetsprinciperna och förfarandena ska åtminstone följande behandlas i praktiken: åtkomsthantering, strukturellt skydd av utrustning och utrustningsutrymmen, tjuvlarm samt övervakning av miljöförhållandena och till exempel användning av släckningsutrustning. Åtkomst bör endast tillåtas för en begränsad mängd personal vars tillförlitlighet och informationssäkerhetskompetens man har säkerställt. I synnerhet åtkomst för tredjepartspersonal ska begränsas och särskilt övervakas.[57]

7. Informationssäker funktion och ändringshantering

Målet med skyldigheterna i punkt 7 i föreskriften är att uppnå bl.a. en spårbarhetskedja för utrustningen och programmen. Programmiljöernas komplexitet gör att spårbarheten

[54] OWASP Cheat Sheet Series, https://cheatsheetseries.owasp.org/.
[55] Punkten baserar sig på informationssäkerhetsmål SO9 enligt ENISA GL, och i genomförandet av det kan de åtgärder som ENISA rekommenderar användas.
[56] Punkt 17.3 i föreskriften om säkerställande av kommunikationsnät och kommunikationstjänster samt om synkronisering av kommunikationsnät förpliktar till skydd av komponenterna i kommunikationsnätet eller -tjänsten fysiskt så att obehöriga inte lätt kommer åt dem.
[57] 5G Toolbox: TM06, s. 25.

är särskilt viktig. För att man ska kunna säkerställa en informationssäker drift av programmiljöer, är det viktigt att veta när ändringar har gjorts, vilka ändringar som har gjorts och vem som har gjort ändringarna.

7.1 Informationssäker användning av kommunikationsnät och -tjänster

Teleföretag ska enligt punkt 7.1.1 i föreskriften ha verksamhetsprinciper och förfaranden för bruket (dvs. funktionen) av komponenter i kommunikationsnätet eller -tjänsten.[58] I fråga om förfarandena kan kravet uppfyllas exempelvis genom att dokumentera ansvaren för driften av nätverks- och informationssystemen och komplettera detta genom att beskriva även de mest centrala rutinerna för hur driften och administrationen av systemen ska genomföras. Det är skäl att regelbundet granska praxis och ansvar samt vid behov uppdatera dem, i synnerhet om det har skett förändringar i miljöerna eller om någon tidigare händelse har visat att det finns brister eller luckor i rutinerna.

7.2 Förändringshantering

Teleföretag ska enligt punkt 7.1.2 i föreskriften ha förfaranden för förändringshantering med hjälp av vilka man minskar sannolikheten för störningar i informationssäkerheten på grund av förändringar, eller vid behov återställer det läge som föregick ändringen eller något annat fungerande läge, med vilka man avser förfaranden för återställande (roll back procedure). Med förändringar avses i detta sammanhang alla förändringar som är väsentliga med tanke på informationssäkerheten och som kan gälla till exempel programvara, hårdvara, konfigurationer och gränssnitt. Förfarandena för förändringshantering kan ställas i relation till de informationssäkerhetsrisker som förändringen medför och som påverkas av förändringarnas art och omfattning.

Beträffande förfarandena för förändringshantering kan kravet uppfyllas genom att dokumentera i förväg fastställda förfaranden för genomförandet av ändringarna.[59] Det är skäl att dokumentationen innehåller en beskrivning av förändringsbehoven, förhandstestningen, produktionstestningen och implementeringen av ändringen i produktionen samt godkännandeförfarandena för varje fas. Som en del av förfarandena för förändringshanteringen är det motiverat att i synnerhet se till de åtgärder som avses i punkt 6.1.2 och 6.1.7 i föreskriften och med vilka komponenterna härdas genom att onödiga behörigheter och tjänster tas bort. Punkt 8.1 i föreskriften gäller testning.

Man ska även planera förfaranden för att upphäva en misslyckad ändring eller avbryta en ändring genom återställande till en version eller konfiguration som man vet att fungerar. Förfarandena för förändringshantering ska omfatta systemens hela utvecklingscykel.[60]

Om hantering av ändringar föreskrivs även i 9 § i Transport- och kommunikationsverkets föreskrift om störningar i televerksamheten. Skyldigheten i fråga har dock inte riktats uttryckligen till att sörja för informationssäkerheten.

[58] ENISA GL SO15.
[59] ENISA GL SO16, 5G Security Control Matrix: M84.
[60] ISO/IEC 27002:2022: 8.32.

7.3 Hantering av egendom och konfigurationer

Teleföretaget ska i enlighet med punkt 7.1.3 i föreskriften ha ändamålsenliga verksamhetsprinciper och förfaranden för hantering av konfigurationer av egendom och komponenter.[61]

Hanteringen av egendom, såsom utrustning och programvara, stöder bland annat hantering av sårbarheter samt prognostisering av beroendeförhållanden och risker. Det är viktigt att hantera konfigurationer för att vid behov kunna återställa rätt inställningar och upptäcka obehöriga ändringar. Det är också bra att observera att det är viktigt att hålla verksamhetsprinciperna och förfarandena uppdaterade efter förändringar och händelser som hotar informationssäkerheten.

Förfarandena bör omfatta ändamålsenliga åtgärder för att förhindra och korrigera obehöriga eller oavsiktliga konfigurationsändringar om konfigurationen är felaktig. Konfigurationshanteringen kan genomföras till exempel med hjälp av särskilda verktyg och genom att föra händelseloggar över ändringar. Hanteringen av egendom och konfigurationer har därför ett nära samband med de förfaranden för förändringshantering som avses i punkt 7.1.2 i föreskriften. Innan ändringarna genomförs är det bra att fastställa förfaranden för att återställa den tidigare versionen (se även kapitel 7.2 i motiveringspromemorian) och att arkivera de gamla versionerna av programvaran som en försiktighetsåtgärd tillsammans med nödvändig information, till exempel detaljer om konfigurationerna och de parametrar som används.[62]

Föreskriftens krav kan beträffande konfigurationer uppfyllas till exempel med en databas för konfigurationshantering (Configuration Management Database, CMDB), med vilken uppgifter om teleföretagets utrustnings- och programegendom förvaltas. Med hjälp av en CMDB är det möjligt att föra bok över de scheman som beskriver nätverkets struktur, komponenterna och programversionerna samt hantera de ömsesidiga beroendeförhållandena mellan komponenterna i kommunikationsnätet och -tjänsten.[63]

I takt med att teleföretagets programmiljö blir mer mångformig är det dessutom viktigt att följa upp och hantera sårbarheterna i programmen på ett systematiskt och centraliserat sätt. Hanteringen av sårbarheter kan därför genomföras som till exempel en proaktiv hantering som baserar sig på olika informationskällor och på en klassificering av komponenterna och sårbarheterna i kommunikationsnätet med hjälp av en materialförteckning av programegendomen (SBOM), varvid det är enklare och snabbare att identifiera och reagera på sårbarheter.[64]

Det är bra att observera, att i Transport- och kommunikationsverkets föreskrift om kommunikationsnätets kritiska delar åläggs teleföretagen skyldighet att identifiera kommunikationsnätets kritiska delar och de komponenter i kommunikationsnätet och -tjänsten som används i dessa. Bestämmelser om skyldigheten att dokumentera uppgifter om alla viktighetsklassificerade komponenter i kommunikationsnäten och -tjänsterna finns i Transport- och kommunikationsverket föreskrift om säkerställande av kommunikationsnät och kommunikationstjänster samt om synkronisering av kommunikationsnät.

[61] ENISA GL SO17.
[62] ISO/IEC 27002:2022: 8.19.
[63] ENISA GL SO17, 5G Security Control Matrix: M88.
[64] Se NIST - Guide to Enterprise Patch Management Planning.SP.800-40r4, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf, SBOM at a Glance (ntia.gov), https://ntia.gov/sites/default/files/publications/sbom_at_a_glance_apr2021_0.pdf och Cybersäkerhetscentret: Hantera sårbarheter säkert med SBOM, https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/hantera-sarbarheter-sakert-med-sbom.

8. Testning och bedömning av informationssäkerheten

Punkt 8 i föreskriften fastställer testning och bedömning av informationssäkerheten.

8.1 Testning av informationssäkerheten i kommunikationsnät och -tjänster samt utförande av säkerhetsbedömningar

Punkt 8.1.1 i föreskriften förutsätter att teleföretaget har ändamålsenliga och uppdaterade verksamhetsprinciper och förfaranden för testning av informationssäkerheten hos komponenter i kommunikationsnät och -tjänster samt för utförande av säkerhetsbedömningar utifrån en riskbedömning. Förfarandena är också en viktig del av förändringshanteringen (punkt 7.2 i föreskriften) och de kan ställas i relation till ändringarnas art och omfattning.

Testning innebär i första hand testning av funktioner som anknyter till informationssäkerheten. Testningen ska verifiera åtminstone säkerhetsfunktionernas korrekthet samt programvaruutvecklingens och konfigurationernas säkerhet.[65] I testningen är det motiverat att utnyttja automatiska testningsverktyg, fastän det kan vara ändamålsenligt att avvika från detta när det gäller till exempel ringa eller annars småskalig televerksamhet. Genomförande av särskilda säkerhetsbedömningar med hjälp av informationssäkerhetsskanningar och till exempel intrångstestning kommer i fråga när det är nödvändigt enligt riskbedömningen.

Testning och säkerhetsbedömningar är viktiga innan nya komponenter och programvaror tas i bruk och innan programvaruändringar görs, för att man ska kunna undvika att störningar och luckor i informationssäkerheten uppstår.[66] Dessutom är det motiverat att med testning och säkerhetsbedömningar efter en ändring försäkra sig om att ändringen inte har orsakat skada för informationssäkerheten. Det kan finnas skäl att genomföra tester och säkerhetsbedömningar under komponenternas hela livscykel för att upptäcka eventuella obehöriga eller oavsiktliga konfigurationsändringar och sårbarheter i komponenterna. På så sätt får man information om informationssäkerhet i nätverket och tjänsterna.

Det är viktigt att utföra testning och säkerhetsbedömning innan nya komponenter tas i bruk och under användningen av dem. Förhandsbedömningen kan bland annat innehålla en kontroll av hur komponenten har härdats, om komponenten har kända sårbarheter i informationssäkerheten och om komponenten har uppdaterats till den senaste ändamålsenliga programvaruversionen. Testning och säkerhetsbedömningar under användningen kan genomföras till exempel genom att skanna komponenterna i nätverket för sådan utrustning och programvaruversioner med kända sårbarheter. Detta förutsätter att sårbarhetsdatabaser som producerats av tredje part används och att resultaten av säkerhetsbedömningen jämförs. Till exempel databasen CVE (Common Vulnerabilites and Exposures) är ett sådant alternativ. Det är rimligt att dokumentera resultaten av säkerhetsbedömningen för att man ska kunna upprätthålla kännedomen om nätverkets informationssäkerhetstatus. Det är bra att resultaten innehåller uppgifter om vilka komponenter som varit föremål för bedömningen, vad som har bedömts, vem som har utfört bedömningen, resultaten av bedömningen samt eventuella fortsatta åtgärder.[67]

[65] ISO/IEC 27002:2022: 8.29.
[66] ENISA GL SO25–SO26.
[67] ENISA GL SO26.

8.2 Bedömningar av informationssäkerheten

Punkt 8.1.2 i föreskriften förutsätter att teleföretag ska ha ändamålsenliga verksamhetsprinciper och förfaranden för att följa upp hur dess informationssäkerhetspolicy och verksamhetsprinciper samt de krav på informationssäkerhet som hänför sig till verksamheten uppfylls.[68]

Regelbunden granskning av kravenlighet stöder säkerheten inom verksamheten och förverkligandet av alla delområden inom informationssäkerheten, när teleföretagets åtgärder för att uppfylla kraven regelbundet granskas på sätt som teleföretaget på förhand bestämmer.

I bedömningarna ska det granskas hur kravenligheten uppfylls förutom i förhållande till den informationssäkerhetspolicy, de verksamhetsprinciper och de förfaranden som teleföretaget själv har fastställt, även i förhållande till de lagstadgade skyldigheter och föreskrifter som gäller informationssäkerhet. Dessutom kan man i bedömningarna granska att tillämpliga standarder följs. Med standarder avses i detta sammanhang sådana standarder som det är obligatoriskt för teleföretaget att följa eller som företaget har förbundit sig att följa som en del av sina metoder för hantering av informationssäkerheten och informationssäkerhetsriskerna.

En sådan här bedömning av informationssäkerheten kan ske genom självbedömning eller genom interna eller externa oberoende bedömningar av informationssäkerheten (kvalitetsrevisioner). Det skulle vara nödvändigt att i verksamhetsprinciper och förfaranden fastställa de bedömningsmetoder som ska användas, det vill säga hur man bedömer kravenligheten, hur ofta man gör bedömningar, hur ofta man registrerar och utför korrigerande åtgärder samt hur man inriktar granskningar eller kvalitetsrevisioner. De kan också fastställa om bedömningarna ska genomföras som förebyggande åtgärder eller eventuellt även efter allvarliga avvikelser i informationssäkerheten eller betydande förändringar.

Enligt föreskriften ska åtminstone resultaten av den senaste bedömningen bevaras.

9. Medvetenhet om hot

Punkt 9 i föreskriften förutsätter att teleföretag har ändamålsenliga tillvägagångssätt för att samla in uppgifter om hot och för bedömning av hot som gäller kommunikationsnätens och -tjänsternas informationssäkerhet. Syftet med denna skyldighet är att teleföretaget ska upprätthålla kontinuerlig, aktuella uppgifter om hot mot komponenter i kommunikationsnätet och -tjänsten. Verksamhetsprinciperna och de närmare förfarandena ska innehålla granskning på en strategisk, taktisk och operativ nivå. De aktuella och bedömda uppgifterna om hot fungerar som viktig utgångsinformation i behandlingen av informationssäkerhetsriskerna.

Det är möjligt för teleföretaget att på ett förebyggande sätt lindra eller avlägsna konsekvenserna av identifierade interna och externa hot på informationssäkerhetsriskerna genom att kontinuerligt vara medvetet om det aktuella hotläget.[69] Eftersom hotmiljön ständigt förändras är det viktigt att medvetenheten om hot utnyttjas i den kontinuerliga

[68] ENISA GL SO27 gäller efterlevnaden av lagstadgade skyldigheter och standarder. Se även ISO/IEC 27002:2022: 5.36, som gäller efterlevnaden av informationssäkerhetspolicyn, verksamhetsprinciperna för informationssäkerheten, regler och standarder.
[69] ENISA GL SO28. Se även ENISA 5G Matrix: M138–M144 och SO29-001–SO29-003, ISO/IEC 27002:2022: 5.6, 5.7 och 8.8), 3GPP TS 33.501, cl. 5.10.1 samt ENISA Report: Cyber Threats Outreach in Telecom, Chapter 4, https://www.enisa.europa.eu/publications/cyber-threats-outreach-in-telecom.

bedömningen av informationssäkerhetsriskerna. I takt med att hotinformationen förändras kan man dessutom identifiera helt nya informationssäkerhetsrisker mot kommunikationsnäten och -tjänsterna.

Insamlingen av uppgifter om hot bör till tillämpliga delar inkludera åtminstone hoten mot programmens och utrustningens leveranskedjor, konsekvenserna av överbelastningsangrepp på funktionen hos kommunikationsnätets- eller tjänsternas komponenter, konsekvenserna av utpressningsprogram och andra skadliga program, sårbarheter i komponenterna, uppföljning av hoten mot BGP-routingen och hot om manipulering av anställda.[70]

Se även kapitel 7.3 i bilagan till motiveringspromemorian (Information om sårbar kundutrustning).

Teleföretagen rekommenderas även att förmedla information om överbelastningsangrepp i Transport- och kommunikationsverkets anmälningsgränssnitt. Syftet med användningen av anmälningsgränssnittet är att samla information om överbelastningsangrepp för att utveckla den allmänna informationssäkerhetsnivån. Med hjälp av denna information kan Transport- och kommunikationsverket exempelvis hjälpa teleföretag att snabbt reagera på hot och störningar i anknytning till överbelastningsangrepp. Datainsamlingen främjar också produktionen av en mer långsiktig lägesbild.

10. Iakttagande av standarder

De nya generationerna av mobilnät utökar nätets tjänster till olika samhällsområden och gör dem till en allt viktigare del av samhällets funktion och annan kritisk infrastruktur. Den nya tjänstebaserade gränssnittsarkitekturen för femte generationens mobilnät ger möjlighet att öppna nätets funktioner för tredje parter samt skapa nya verksamhets- och tjänstemodeller. Samtidigt används äldre webbgenerationer, av vilka i synnerhet 4G-nätet fortfarande används länge tillsammans med 5G-nätet. Samtidigt ökar dock hanteringen och öppnandet av gränssnitten komplexiteten och hotytan. I sådana fall är det särskilt viktigt att samtliga säkerhetsfunktioner i nätverksutrustningen observeras och att de utnyttjas i så stor utsträckning som det inom teleföretagets verksamhet är nödvändigt.

Punkt 10.1 i föreskriften förutsätter att teleföretaget i mobilnätet använder ändamålsenliga förfaranden genom vilka det säkerställer att alla nödvändiga säkerhetsfunktioner i 4G-, 5G- och IMS-systemen enligt de tekniska specifikationerna i bilaga 1 till föreskriften förverkligas.

Med förverkligande av säkerhetsfunktionerna avses förutom att de komponenter som används i kommunikationsnätet och -tjänsten stöder funktioner i enlighet med dessa standarder, även att funktionerna tas i bruk i teleföretagets kommunikationsnät. Genom förfarandena bör säkerhetsåtgärdernas beständighet säkerställas även i samband med programuppdateringar och genomförandet av nya funktioner.

3GPP utarbetar sina tekniska specifikationer och standarder till versioner (release), vars införande ibland kan ta lång tid och framskrida stegvis i nätet. Funktioner som definieras i en senare version kan ibland även genomföras och införas delvis i situationer där en komponent i kommunikationsnätet eller -tjänsten till övriga delar ännu genomför en

[70] Se ENISA Threat Landscape for Supply Chain Attacks, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks, ENISA Threat Landscape 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 och ENISA Threat Landscape for 5G Networks Report, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks.

äldre version. Därför är det skäl att bland versionerna av tekniska definitioner alltid granska en version som godkänts av 3GPP och som motsvarar den version av funktionaliteten som genomförs i teleföretagets nät.

Teleföretag kan låta bli att uppfylla det säkerhetskrav som anges i första punkten, i det fall att det inte är ändamålsenligt med beaktande av dess betydelse för kommunikationsnätets eller -tjänstens informationssäkerhet och övriga till saken anknutna åtgärder för att ombesörja informationssäkerheten i det aktuella fallet (punkt 10.2 i föreskriften). Grunden för att låta bli att genomföra en säkerhetsfunktion i enlighet med en standard kan vara till exempel genomförande av en alternativ säkerhetsfunktion som tillräckligt väl minskar risken som de identifierade hoten medför. Exempelvis avsaknad av en säkerhetsfunktion i en utrustning, ett program eller en del av ett sådant, utrustningens logiska eller fysiska läge samt ett behov som hänför sig till hanteringen av eller observationer i nätet kan vara en grund för att låta bli att genomföra en valfri säkerhetsfunktion antingen tillfälligt eller vid behov permanent på ett sätt som riskbedömningen kräver. I riskbedömningen ska hoten mot både teleföretaget och kommunikationstjänstens användare beaktas.

I enlighet med punkt 10.3 i föreskriften ska teleföretaget upprätthålla en beskrivning av de förfaranden genom vilka det säkerställer att säkerhetskraven i standarderna uppfylls. Dessutom är kravet att underlåtenheten att genomföra varje säkerhetsfunktion eller säkerhetsmekanism på grundval av punkt 10.2 dokumenteras separat. Syftet med detta krav är att möjliggöra övervakning av skyldigheten och att grunderna för tillämpningen av undantaget kan verifieras i efterhand.

Föreskriften förutsätter inte att teleföretaget till exempel genom egna åtgärder testar hur väl genomförandet av samtliga funktioner överensstämmer med standarderna, utan de ändamålsenliga förfarandena kan inkludera till exempel krav i frågan som ställs på leverantören av utrustningen och vilkas uppfyllande följs upp genom lämpliga åtgärder. Teleföretaget kan om det är möjligt även som en del av förfarandena utnyttja informationssäkerhetscertifieringen i enlighet med EU:s cybersäkerhetsförordning när den bli tillgänglig[71] eller en bedömning av komponenterna i enlighet med NESAS-schemat[72]. Utöver detta ska man genom förfarandena även sörja för att säkerhetsfunktionerna införs och upprätthålls på korrekt sätt som en del av konfigurationshanteringen av komponenterna.

11. Datamaterial

För att information med anknytning till televerksamheten ska vara tillgänglig endast för dem som har rätt att använda den, ska teleföretag ha ett klassificeringssystem, klassificeringskriterier och hanteringsförfaranden i samband med klassificeringen av sådant datamaterial som är viktigt för televerksamheten.

Klassificeringen och hanteringen av datamaterial hänger även nära samman med åtkomstkontrollen av användarna i enlighet med klassificeringen av datamaterial.

Åtkomstkontrollen av användare behandlas i punkt 6.1.1 i föreskriften.

[71] ENISA Securing EU's Vision on 5G: Cybersecurity Certification, https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification.
[72] GSMA Network Equipment Security Assurance Scheme (NESAS), https://www.gsma.com/security/network-equipment-security-assurance-scheme/.

Teleföretag ska fastställa sådana kriterier för klassificeringen av datamaterial som lämpar sig för dess verksamhet. Materialet kan exempelvis klassificeras på följande sätt: offentligt, konfidentiellt och sekretessbelagt.

Dessutom ska teleföretaget fastställa på vilket sätt företaget hanterar (skyddar) materialet som har indelats i olika klasser.

Klassificeringen och de tillhörande anvisningarna för hantering av datamaterial ska dokumenteras (se punkt 3.2 i föreskriften). Faktorer som ska beaktas när klassificeringen fastställs och dokumenteras är exempelvis följande:

- allmänna principer för bedömning av datamaterialets säkerhetsklass och konfidentialitet samt hemlighållandet av datamaterial
- hanterings- och ändringsrättigheter vad gäller fördelningen av läsrättigheter till datamaterialet, ändringsrättigheter och fördelningen av dessa rättigheter
- fastställande av konfidentialitetsklass
- offentlighet av uppgifter eller dokument: till exempel rätten att tala om ett ärende offentligt
- dokumentets egenskaper: papper, stämpel och andra märkningar
- förvaring och kryptering
- utskrifter och kopiering
- säkerhetskopiering
- mottagning, distribution, sändning och transport
- dokumentering av hanteringen av uppgifter och dokument
- arkivering och hantering av dokument eller upphörande av hanteringsrätten samt förstöring av uppgifter och dokument.

12. Identifiering av kund i syfte att sköta om informationssäkerheten

Punkt 12 i föreskriften förutsätter att teleföretaget har ändamålsenliga verksamhetsprinciper och tillvägagångssätt för att kunna identifiera abonnenten eller användaren på ett tillräckligt tillförlitligt sätt innan ändringar som påverkar kommunikationstjänstens informationssäkerhet utförs på kundens tjänst eller innan abonnenten eller användaren får konfidentiella uppgifter. Den metod som används för identifieringen kan ställas i relation till ärendehanteringens risknivå med tanke på de ändringar som görs i tjänsten eller vilka konfidentiella uppgifter som ges ut. När risknivån bedöms ska man förutom att utvärdera kundhändelsen även beakta beställarens eller användarens särdrag, såsom eventuella förbud mot att lämna ut uppgifter. I verksamhetsprinciperna och förfarandena kunde man till exempel fastställa tillräckliga identifieringsförfaranden på riskbaserad basis för olika ändringar i tjänsten och kunduppgifter.

Det är skäl att de upprättade verksamhetsprinciperna och tillvägagångssätten ingår i utbildningsprogrammet för personal som deltar i kundservicen. I punkt 5 i föreskriften åläggs teleföretag skyldighet att se till att personalen har behövliga kunskaper i informationssäkerhet och regelbundet ordna utbildning i informationssäkerhet. Krav som gäller personalens kunskaper i informationssäkerhet och utvecklingen av dem ställs i punkt 5.1.2.

Ett tillförlitligt sätt att inom *elektronisk kommunikation* identifiera abonnenten eller användaren kan anses vara till exempel användning av stark autentisering som avses i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009). Ett alternativt tillförlitligt sätt att identifiera abonnenten och användaren kan med beaktande av

risknivån vara användning av tvåfaktorsautentisering exempelvis med en mobilapplikation. Vid *ärenden som uträttas genom besök* kan ett tillförlitligt sätt vara att till exempel kontrollera abonnentens eller användarens identitetshandling. Tillförlitliga identitetshandlingar är till exempel ett finländskt pass, identitetskort eller körkort samt utländska handlingar med en jämförbar tillförlitlighet, såsom ett pass eller ett identitetskort som beviljats av en stat inom Europeiska ekonomiska samarbetsområdet. En handling ska inte godkännas om inte teleföretaget med tillräcklig säkerhet kan fastställa att handlingen verkligen tillhör den person som uppvisar den, eller om det finns skäl att misstänka att handlingen är förfalskad.[73] Även vid *telefonkommunikation* ska kunden kunna identifieras på ett tillräckligt tillförlitligt sätt. På basis av en riskbedömning är det möjligt att vid telefonkommunikation identifiera kunden på ett tillräckligt tillförlitligt sätt till exempel med hjälp av en lista med frågor, som ingen utomstående känner till svaren på. Dessutom kan man vid telefonkommunikation i den mån det är möjligt använda stark autentisering eller en mobilapplikation.

Som väsentliga ändringar som görs i tjänsten och som påverkar kommunikationstjänstens informationssäkerhet kan betraktas åtminstone byte av SIM-kort för abonnemanget, återöppnande av ett abonnemang (utlämnande av PUK-kod), upprättande eller aktivering av ett eSIM samt stängning av ett abonnemang.[74] Väsentliga ändringar är även byte av ett glömt lösenord för ett e-postkonto eller öppnande av ett låst användarkonto. Som konfidentiella uppgifter betraktas bland annat förmedlingsuppgifter om abonnenten eller användaren, till exempel uppgifter i en detaljerad fakturaspecifikation, eller uppgifter som sparats i en e-post- eller snabbmeddelandetjänst. Teleföretaget ska inte göra väsentliga ändringar i tjänsten och inte lämna ut konfidentiell information om tjänstens abonnent eller användare inte har identifierats på ett tillräckligt sätt.

13. Dokumentation av IP-adresser

Punkt 13 i föreskriften förutsätter att teleföretaget på behörigt sätt ska dokumentera användningen av de IP-adresser som är adresserade till teleföretaget och som annonseras av teleföretaget genom att registrera IP-adresserna i databasen för den internet-registrator (IR) som överlåtit adresserna eller någon annan adekvat internet-registrator. Detta är viktigt, eftersom teleföretagen kan använda dessa uppgifter för att skapa till exempel automatiska listor för filtrering av rutter (prefix list). Med listorna försäkrar man sig om att det teleföretag som annonserar rutterna endast annonserar de adressrymder som det förfogar över. IP-nätresurser som har dokumenterats på behörigt sätt gör det också mycket lättare att upprätthålla routinginformation och att undersöka störningar och informationssäkerhetskränkningar.

Teleföretaget ska anmäla de nätverk som det förvaltar till WHOIS-databasen hos en ändamålsenlig internet-registrator (IR). Med förvaltade nätverk avses i anknytning till föreskriften de domäner som ägs av teleföretaget eller levereras till dess kunder. Uppgifterna registreras och upprätthålls i enlighet med registratorns anvisningar. Uppgifter som ska registreras är bland annat IP-adressrymd, teleföretagets kontaktuppgifter, kontaktuppgifter för den som upprätthåller databasen, abuse-och irt-kontaktuppgifter samt nätets AS-nummer där de relevanta IP-adresserna finns. RIPE NCC, som är en internetregistrator i Europaområdet, använder ett särskilt datafält för registrering av abuse-kontakter.

[73] Om godkännande av en handling som beviljats av någon annan än en finsk myndighet se HFD 2017:19, https://www.kho.fi/sv/index/beslut/arsboksbeslut/1486031131275.html.
[74] Se SIM-ENISA Countering SIM-Swapping, s. 17–20, om förfaranden för att bekämpa bedrägerier med SIM-kortutbyte, https://www.enisa.europa.eu/publications/countering-sim-swapping.

Teleföretaget ska i synnerhet se till att dokumentationen över de IP-nät som teleföretaget använder hålls uppdaterade. Om teleföretaget utgör en källa för ruttannonsering för PI-nätverksrymder (Provider Independent) som andra organisationer innehar, ska teleföretaget kontrollera vederbörligheten av uppgifterna om adressrymder i samband med aktiveringen av ruttannonseringen. Likaså ska uppgifternas korrekthet granskas vid registreringen av adressrymden om teleföretaget upprätthåller en lokal internetregistratorstjänst (LIR) och överlåter PI-adressrymd till tredje parter.

I praktiken betyder kravet också att teleföretaget inte får annonsera odokumenterade IP-adressrymder för andra teleföretag, om inget annat uttryckligen har avtalats.

14. Trafik mellan hanteringsnät och hanteringsförbindelser

Teleföretaget ska ha ändamålsenliga verksamhetsprinciper och praxis som gäller nätverksadministration och administrationsförbindelser med hjälp av vilka man säkerställer att en säkerhetsnivå i enlighet med riskbedömningen genomförs för att minimera informationssäkerhetshoten (punkt 14.1 i föreskriften). Föreskriften förutsätter att teleföretaget ska skydda den s.k. kontrolltrafiken för kommunikationsnätets eller -tjänstens komponenter (punkt 14.2 i föreskriften). Med kontrolltrafik avses trafik genom vilken teleföretaget övervakar och administrerar sin nätutrustning. Syftet med kravet på att skydda kontrolltrafik är att säkerställa att ingen obehörigt kan göra ändringar i ett kommunikationsnäts eller en -tjänsts komponenter.

Verksamhetsprinciperna ska innehålla åtminstone krav för skyddet av kontrolltrafiken, härdningskrav för terminalutrustning som används för nätverksadministration samt principer för åtkomsthantering utifrån hur centrala komponenter i kommunikationsnätet och -tjänsterna som det är fråga om.

I praktiken kan kontrolltrafiken skyddas genom att skilja trafiken från varandra fysiskt med egna ledningar för trafiken eller logiskt exempelvis genom trafikkryptering. Det är nödvändigt att kryptera kontrolltrafiken med en metod som lämpar sig för användningssituationen i synnerhet om det inte annars är möjligt att säkerställa att följning eller kapning av trafiken har förhindrats. Okrypterad kontrolltrafik kan avslöja information om eller egenskaper hos komponenter i ett kommunikationsnät eller en kommunikationstjänst.

Dessutom ska teleföretag använda behövliga förfaranden för att bedöma hot mot informationssäkerheten som orsakas av terminaler som används för nätverksadministration och för att hantera risker orsakade av dessa (punkt 14.3 i föreskriften). Särskild uppmärksamhet ska ägnas åt skyddet av terminalutrustning som används för hantering av komponenterna i kommunikationsnätet och -tjänsterna, eftersom informationssäkerhetshot även riktar sig mot hanteringsnätet via dessa tjänster, om exempelvis e-post och internettjänster kan användas med samma terminalutrustning.

I en del situationer kan man använda en dedikerad, härdad arbetsstation, varvid möjligheten att på terminalutrustningen använda andra funktioner än de som är nödvändiga för nätverksadministrationen elimineras. Inom riskhanteringen kan man utifrån en helhetsbedömning även använda andra tillvägagångssätt, där riskerna som beror på terminalutrustningen har hanterats på andra sätt. Utgångspunkten för föreskriften är att terminalutrustning som används för nätverksadministration inte ska anslutas direkt till systemen i hanteringsnätet, utan användningen av hanteringsnätet bör genomföras till exempel som virtuellt terminerad, genom förmedling av en noggrant övervakad hoppmaskin, eller med hjälp av en lösning som baserar sig på ett fjärrskrivbord. Enbart

tvåfaktorsautentisering, virusskydd eller en VPN-anslutning bör inte anses vara tillräckligt. Vid överföring av nödvändiga filer från en terminalenhet till en annan ska man också ta hänsyn till risk för skadliga program bl.a. genom att endast använda tillförlitliga källor och säkerställa informationssäkerheten (integriteten) med alla nödvändiga metoder.

I åtkomsthanteringen av förbindelser i hanteringsnätet ska principen om lägsta behörighet utan undantag tillämpas, och identifieringen av användarna ska ske med åtminstone två autentiseringsfaktorer. Sändning av en autentiseringsfaktor per SMS bör inte vara det primära sättet. Därtill ska lämpliga förfaranden genomföras och dokumenteras genom vilka de kvarstående riskerna som hänför sig till säkerställandet av hanteringsförbindelsens informationssäkerhet minskas. Förfarandena kan till exempel omfatta att begränsa anslutningar till vissa IP-adresser, tillåta hanteringsanslutningar på behovsbasis, begränsa varaktigheten av händelser, övervaka i realtid och logga hanteringsanslutningar.

Kraven som gäller åtkomstkontrollen av användare behandlas även i punkt 6.1 i föreskriften.

Rekommendation

Transport- och kommunikationsverket rekommenderar att teleföretaget upprätthåller en logg över de ändringar som gjorts i inställningarna för sin nätutrustning under det senaste halvåret för att upptäcka och spåra eventuella obehöriga ändringar i nätutrustningens inställningar. Verket rekommenderar också att tidsanteckningarna för en loggad händelse och observation anges separat för händelsen och observationen. Det rekommenderas att tidpunkten för observationen loggas med åtminstone exakt datum, och i systemloggar som beskriver händelsen ska även exakt klockslag, tillämplig tidszon (t.ex. UTC+2) samt storleken och riktningen på eventuella klockfel jämfört med den officiella tiden sparas. De tekniska systemloggarnas tidsstämplar ska ges i ett format som överensstämmer med ISO 8601.[75]

Kapitel 3 Särskilda krav på kommunikationsnät och -tjänsternas gränssnitt

Detta kapitel behandlar de krav som i föreskriftens kapitel 3 ställs på informationssäkerheten i samtrafik-, tillämpnings- och kundgränssnitt.

15. Förhindrande av och skydd mot störningar i gränssnitten

15.1 Förhindrande av störningar

Teleföretagets nät eller tjänst får inte orsaka störningar för andra kommunikationsnät eller -tjänster. Förpliktelsen som åläggs i punkt 15.1 i föreskriften förbjuder även avsiktlig störning, men kravet är ändå i första hand avsett för att förebygga oavsiktlig spridning av störningar från ett nät till ett annat, till exempel sådana som ett konfigureringsfel orsakar. Störningar som sprids över samtrafikgränssnittet kan bilda slingor i nätet, styra trafik till fel adress eller bara belasta en del av nätet eller tjänsten med extra trafik. I värsta fall kan användningen av tjänsten förhindras helt.

[75] En rekommendation med motsvarande innehåll har getts i punkt 9.2 i motiveringspromemorian till föreskrift 66 A/2019 M om störningar i televerksamheten.

Eftersom sådana störningar kan medföra betydande verkningar, har det ansetts vara nödvändigt att ålägga teleföretag skyldighet att se till att dess egna kommunikationsnät eller -tjänst inte stör de övriga kommunikationsnätens tjänster. Skyldigheten har ålagts trots att även punkt 15.2 i föreskriften innehåller en skyldighet för teleföretaget att skydda sig mot sådana störningar.

Kravet har inte riktats mot en viss teknik eller protokollnivå, utan teleföretaget ska bedöma vilka hot de olika tekniker och tjänster som används i samtrafikgränssnittet kan orsaka och sedan genomföra alla skyddsmekanismer som behövs för att teleföretaget ska kunna förebygga störningar.

Ett exempel på nödvändiga skyddsmekanismer är mekanismer med vilka man förebygger slingor i samtrafikgränssnitten. Till exempel i kretskopplade telefonitjänster får samtalet vidarekopplas högst fem gånger, varefter samtalet kopplas ned. Vid sammankoppling av internetaccesstjänster avses med detta att teleföretaget inte över samma logiska gränssnitt skickar sådan trafik som det har tagit emot över detta gränssnitt.

Även om föreskriften i övrigt tillämpas endast på allmän televerksamhet, är det bra att observera att skyldigheten att förhindra störningar enligt punkt 15.1 i föreskriften också gäller myndighetsnät och kommunikationstjänster i anslutning till myndighetskommunikation till den del de är sammankopplade med ett allmänt kommunikationsnät eller en allmänt tillgänglig kommunikationstjänst, det vill säga ett teleföretags nät eller tjänst. Den aktör som tillhandahåller och upprätthåller ett myndighetsnät eller en kommunikationstjänst i anslutning till myndighetskommunikation omfattas därmed av en skyldighet att se till att komponenterna i dess kommunikationsnät eller -tjänst inte orsakar störningar för allmänna kommunikationsnät. En sådan aktör ska ha ändamålsenliga mekanismer för att förhindra störningarna i fråga.

I kapitel 6 i bilagan till denna motiveringspromemoria ges rekommendationer om informationssäkerheten i Ethernet-teknik.

15.2 Skydd mot störningar

Enligt punkt 15.2 i föreskriften ska företaget skydda sitt eget kommunikationsnät och sina -tjänster mot skadlig trafik från samtrafik-, tillämpnings- och kundgränssnitt med hjälp av behövliga skyddsmekanismer för nätet.

Jämfört med samtrafikgränssnitten mellan kommunikationsnät är hoten i kundgränssnitt ännu mångsidigare. Teleföretagen ska t.ex. i fråga om internetaccesstjänster bl.a. se till att kunden inte kan avlyssna andra kunders trafik eller rikta blockeringsattacker mot dessa. Hotens kvalitet och storlek samt nödvändiga skyddsåtgärder varierar enligt den tjänst som tillhandahålls och den teknik som används.

Med skadlig trafik som nämns i samband med skyldigheten avses i detta fall i huvudsak trafik som är skadlig för teleföretagets eget kommunikationsnät eller -tjänst och som i värsta fall kan äventyra kommunikationsnätets eller -tjänstens funktion.

Kravet har inte riktats mot en viss teknik eller protokollnivå, utan teleföretaget ska bedöma vilka hot som de olika tekniker och tjänster som används vid gränssnittet kan orsaka och sedan genomföra alla skyddsmekanismer som behövs för att teleföretaget ska kunna skydda sina kommunikationsnät och tjänster. Exempel på sådana mekanismer är filter som baserar sig på käll- eller måladress, använt protokoll, meddelandets innehåll eller antalet meddelanden.

Dessa skyddsmekanismer kan genomföras även på kontrollnivå, och då är det inte nödvändigt att filtrera meddelanden. Mot vissa hot kan det räcka att teleföretaget endast skyddar kontrollnivån för den utrustning som behandlar trafiken i fråga och sedan förmedlar trafiken normalt genom nätet. Om teleföretaget skyddar kontrollnivån i stället för att filtrera trafiken, ska företaget naturligtvis genomföra de behövliga mekanismerna i alla nödvändiga nätelement.

Nedan finns några exempel på hot och skyddsmekanismer som då behövs. Det bör beaktas att exemplen inte är uteslutande och att teleföretaget måste överväga vilka åtgärder som behövs.

- Kundgränssnitt för bitström: En nätoperatör ska exempelvis filtrera BPDU-meddelanden (Bridge Protocol Data Units) som kommer till och utgår från kundporten i kundgränssnittets Ethernet-DSLAM (Digital Subscriber Line Access Multiplexer) eller i bakomliggande kantswitch samt tillverkarspecifika styrprotokollmeddelanden på nivå L2.
- Kund-och samtrafikgränssnitt för VoIP: Problemet har behandlats närmare i exempelvis RFC 5390[76] och 6404[77]. Andra eventuella nödvändiga skyddsåtgärder är t.ex. begränsningar som baserar sig på källadresser eller antal samtalsförsök. Dessa mekanismer kan genomföras med hjälp av SBC[78].

16. Stängning av onödiga portar, tjänster och protokoll

Det är väsentligt att sådana tjänster och protokoll som är onödiga med tanke på kommunikationstjänsternas och teleföretagets systems funktion stängs av eller blockeras från komponenterna i kommunikationsnätet eller -tjänsten, eftersom kommunikationsnätets eller -tjänstens komponent då kör färre program vars sårbarheter en eventuell angripare kan utnyttja. Filtrering av obehövliga routingprotokoll eller övrig styrtrafik i administrationsgränssnitten minskar dessutom möjligheten att trafik som kommer över gränssnittet ska kunna störa funktionen hos teleföretagets nät.

Kravet tillämpas på komponenter i kommunikationsnät eller -tjänster i både samtrafiks- och kundgränssnitt (dvs. inte på kundterminalutrustning, t.ex. modem, switchar, datorer etc. som en kund äger och förfogar över). Kravet är inte riktat direkt mot en viss teknik eller protokollnivå, utan teleföretaget ska för varje utrustning och eventuellt även för varje port överväga vilka fysiska portar, kommunikationsportar (t.ex. portar för TCP- och UDP-protokoll) eller tjänster som är obehövliga och koppla bort dem. Skyldigheten gäller däremot inte allmänt kommunikationsportar som är tillgängliga i trafiken i en kundanslutning till en internetaccesstjänst.

I en del utrustning kan detta ha beaktats redan i standardinställningarna eller så kan tillverkaren tillhandahålla kommandon med vilka många sådana tjänster kan kopplas bort på en gång. Teleföretaget ska undersöka det lämpligaste sättet för varje utrustning, eftersom man inte kan utgå ifrån att frågan gällande obehövliga tjänster och protokoll alltid är i ordning.

[76] IETF RFC 5390, Requirements for Management of Overload in the Session Initiation Protocol, https://tools.ietf.org/html/rfc5390.
[77] IETF RFC 6404, Session PEERing for Multimedia INTerconnect (SPEERMINT) Security Threats and Suggested Countermeasures, https://tools.ietf.org/html/rfc6404.
[78] IETF RFC 5853, Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC) Deployments, https://tools.ietf.org/html/rfc5853.

Nedan följer några exempel på hur skyldigheten kan fullgöras i olika nätelement. Det bör beaktas att exemplen inte är uteslutande och att teleföretaget måste överväga vilka åtgärder som behövs.

- Kundgränssnitt för bitström (PE-router): Det betyder till exempel att FTP-, HTTP-, NTP-, finger- eller bootp-tjänster inte är påslagna i PE-routerns kundport i kundgränssnittet. På kontrollnivå ska det likaså inte behandlas meddelanden om routingportar eller proxy-arp som kommer från kundportar. Det är dock möjligt att förmedla trafik genom nätet.
- Server för sändning av e-post (MSA): Server för sändning av e-post är en anordning eller en virtuell server i kundgränssnittet genom vilken e-postmeddelanden skickas vidare. En sådan server behandlar inte routing- eller övriga styrprotokoll på nätverksnivå. För att sårbarhetshoten ska kunna minimeras får man i ett sådant nätelement inte ha onödiga tjänster påslagna, som för MSA kan vara exempelvis FTP- eller HTTP-servrar.

17. Skydd av IP-samtrafikgränssnitt och filtrering av trafiken

Informationssäkerheten i routingprotokoll

Internetstamnätets centrala routingprotokoll BGP (Border Gateway Protocol) saknar som standard en inbyggd säkerhet, vilket utsätter det för konfigurationsfel och angrepp. BGP är ett samtrafikprotokoll som organisationer använder för att ansluta sitt nät till övriga internet för att å ena sidan skicka trafik till rätt destination och å andra sidan ta emot trafik, som är avsedd för objekt i organisationens egna IP-adresser.

Av ovanstående orsaker har Transport- och kommunikationsverket ansett att det är nödvändigt att införa skyldigheter för att förbättra routingens informationssäkerhet. De skyldigheter som åläggs i föreskriften baserar sig till största delen på ENISAs rekommendationer för att skydda routingprotokollet BGP.[79]

Aktörers nätverkshelheter som är kopplade till internet kallas autonoma system (Autonomous System, AS). Varje autonomt system har en individuell nummerkod (ASN), som kännetecknar respektive AS på internet. Nummerkoderna på internet delas ut av organisationen Internet Assigned Numbers Authority (IANA) och de regionala internetregisterorganisationer (Regional Internet Registry, RIR) som verkar under den. Varje autonomt system kontrollerar en eller flera särskilda grupper IP-adresser och har kontakt med flera andra AS-system, till vilka det med hjälp av BGP-protokollet meddelar de adresserier som det administrerar. Denna information används för att styra nättrafiken bestående av datapaket till rätt objekt, det vill säga till den aktör som administrerar de adresser som är målet.

BGP-protokollet utarbetades för över 25 år sedan enligt verksamhetsprinciperna enkelhet, enkelt ibruktagande samt driftssäkerhet och flexibilitet, vilket har bidragit till att protokollet används ännu i dag. Internets roll och storlek var på den tiden mindre än i dag, och det var endast ett litet antal aktörer som kände varandra som utbytte rutter sinsemellan. Aktörerna hade förtroende för varandra, och därför ansågs det inte nödvändigt att lägga vikt vid säkerhetsaspekter. BGP baserar sig således framför allt på en tillit till att de data som tas emot är korrekt. De noder som ska routas, dvs. routerenheterna, publicerar information om dataöverföringsvägarna till andra routrar, och de andra routrarna litar på den erhållna informationen och sprider den vidare utan kontroller. I takt med att internetanvändningen blivit vanligare och tjänster övergått till nätet

[79] ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP), https://www.enisa.europa.eu/publications/7-steps-to-shore-up-bgp.

har antalet aktörer ökat explosionsartat, varför konfigurationsfel och mänskliga misstag möjliggör uppkomsten av också omfattande störningar. Bland de som utbyter rutter kan det också finnas illasinnade aktörer, som vill förfalska ruttinformation för sina egna användningsändamål, t.ex. för att stjäla trafik och informationen som den innehåller, försöka orsaka avbrott i vissa tjänster eller styra trafik till fel ställe i bedrägerisyfte.[80]

Kapning av rutter är ett av de vanligaste problemen i fråga om säkerheten i BGP. Vid en kapning börjar en nod som ska routas annonsera felaktig information om rutterna till de grannoder som är direkt anslutna till den eller alternativt annonsera att den äger vissa IP-adresser som egentligen hör till någon annan aktör. BGP innehåller i sig inget kontrollförfarande för detta beteende, vilket innebär att sådan felaktig information också på mycket kort tid kan hinna sprida sig till en stor del av internet och göra så att trafik styrs fel samt att tillgången till och användningen av tjänster kanske förhindras.

BGP är utsatt även för andra informationssäkerhetshot förutom kapning av rutter. För upprättandet av BGP-sessioner mellan två aktörer används TCP/IP-protokoll. Angriparen kan försöka till exempel ändra icke-hierarkisk kommunikation i BGP genom att mata in förfalskade BGP-meddelanden i kommunikationen mellan BGP-partner i syfte att bryta eller ändra förbindelsen för att störa, kapa eller skriva om internettrafiken.

Felaktiga käll-IP-adresser

IP-paket som sänds till teleföretagets nät och dess abonnenter kan innehålla en felaktig källadress som definierats så av misstag eller med avsikt. Om teleföretaget tar emot IP-paket vars källadress är teleföretagets egna adresser (adresser som det självt förfogar över) eller adresser som hör till en privat (icke-offentlig/icke-routad) IP-adressrymd från ett annat teleföretag, utan separat avtal, är det en onormal situation och innebär en betydande informationssäkerhetsrisk. Utöver ovanstående finns det även andra adresser som aldrig borde förekomma i routing. Exempel på sådana är domäner som regionala internetregister (RIR) ännu inte har fördelat och domäner som är avsedda för särskilda ändamål.

Förfalskade käll-IP-adresser (IP spoofing) används ofta vid överbelastningsangrepp. Angreppet görs så att angriparen förfalskar sin egen nätadress så att den som utsätts tror att IP-paketen kommer från en tillförlitlig källa. Förfalskade källadresser används för att dölja angriparen. Om filtrering av IP-paket som skickats med förfalskad avsändaradress saknas, kan andra internetanvändare bli utsatta för skada utan möjlighet att utreda vem som står bakom angreppet. Syftet med kraven för felaktiga källadresser är att avsevärt begränsa problem som orsakas av angrepp som begås med förfalskade käll-IP-adresser och felsituationer i nätet.

17.1 Upptäckt av avvikelser i routing

Med avvikelse i routing avses en onormal och ofta också plötslig förändring av informationen om nätets tillgänglighet och topologi, som kan ha negativa konsekvenser för förmedlingen av internettrafiken. Det är viktigt att observera en avvikelse i routing för att upprätthålla en lägesbild av förändringar som kan skada teleföretagets egen näthelhet. Vikten av att upptäcka samt möjligheten att reagera på avvikelser är särskilt stor i synnerhet med tanke på att angrepp mot BGP-protokollet kan leda till stora konsekvenser för nättrafiken. Dessutom möjliggör monitoreringen och observationen analyser på längre sikt, med hjälp av vilka man kan planera förebyggande åtgärder för att upprätthålla säkerheten i nättrafiken.

[80] ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP).

Föreskriften förutsätter att teleföretaget har förmåga att upptäcka avvikelser som är synliga i de egna rutterna. Beträffande de egna rutterna ska man åtminstone kunna upptäcka hur de rutter som teleföretaget annonserar syns utanför teleföretagets egen omgivning (dvs. ute i världen), så att man till exempel kan upptäcka en situation där någon annan börjar annonsera en konkurrerande rutt till näten i fråga av misstag eller för illvilliga ändamål. För att genomföra observationen kan man utnyttja till exempel offentliga servrar för routing data, såsom data som samlats in av RIPE NCC Routing Information Service[81].

Teleföretaget bör även monitorera och övervaka BGP-nättrafik som kommer från andra nätverkshelheter och skickas ut från teleföretagets egen nätverkshelhet, så att teleföretaget kan upprätthålla sin kännedom om såväl den egna nätverkshelhetens stabilitet och resiliens som sina abonnenters integritet och informationssäkerhet.

17.2 Skydd av BGP-sessioner

Föreskriften förutsätter att teleföretaget skyddar sådana BGP-sessioner som används för utbyte av routinginformation med routinggrannar alltid när det är möjligt. Skyddet av TCP-sessioner i BGP kan genomföras exempelvis med hjälp av de lösningar som beskrivs i IETF:s definition RFC 5925[82]. Förfalskning av BGP-sessioner kan i sin tur förhindras genom till exempel användning av en allmän TTL-skyddsmekanism (Generalized TTL Security Mechanism, GTSM[83]). I en GTSM används antingen livslängden för ett IPv4-paket (Time to Live, TTL) eller hoppgränsen i ett IPv6-paket (eng. hop limit) för att kontrollera huruvida paketet har skickats av en nod bredvid den sammankopplade länken, det vill säga den granne med vilken BGP-sessionen har upprättats. GTSM-lösningen beskrivs i IETF:s definition RFC 5082[84].

Målet med skyldigheten att skydda sessioner är bl.a. att förhindra avbrott i BGP-sessioner med hjälp av ett man-in-the-middle-angrepp eller inmatning av felaktig information i sessioner.

Ibruktagandet av ovanstående säkerhetsåtgärder kräver konfigurationsändringar inte bara på lokala routerenheter utan även på routerenheter hos en trafikutbytespartner. En teleoperatör kan ha partnerskap för trafikutbyte med andra än andra teleoperatörer, och i sådana fall är det inte nödvändigtvis möjligt att komma överens om att ta i bruk skyddsåtgärder. I så fall ska teleföretaget i vilket fall som helst göra det möjligt att skydda BGP-sessionerna och för sin del sträva efter att främja ibruktagandet av skyddsåtgärder, men om en viss åtgärd inte kan avtalas med en trafikutbytespartner är det naturligtvis inte möjligt att genomföra skyddet i fråga.

17.3 Filtrering av felaktiga källadresser

Föreskriften förutsätter att teleföretaget filtrerar trafik som kommer till företagets kommunikationsnät och har en felaktig käll-IP-adress, om man inte har kommit överens om något annat. Det rekommenderas att teleföretaget i routrar använder speciella filter som gör det möjligt att minska antalet IP-paket med förfalskade adresser både för inkommande och utgående trafik.[85]

[81] RIPE NCC, https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris
[82] IETF RFC 5925, The TCP Authentication Option, https://tools.ietf.org/html/rfc5925
[83] ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP), s. 12 (TTL Security (GTSM)
[84] IETF RFC 5082, The Generalized TTL Security Mechanism (GTSM), https://tools.ietf.org/html/rfc5082
[85] ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP). Se även MANRS Actions for Network Operators, Action 2. Version 2.5.2 – 17 May 2021, https://www.manrs.org/netops/network-operator-actions/.

Kravet gäller endast källadresser som med tanke på teleföretagets nät är signifikanta, dvs. teleföretaget behöver inte kontrollera t.ex. andra källadresser i IP-paketens nyttolast som förmedlas i samband med VPN-tunnlingen.

Filtreringsåtgärderna ska vidtas med tekniskt ändamålsenlig precision i samtrafikgränssnittet. Eventuella lösningar och faktorer som ska beaktas beskrivs i IETF:s specifikationer RFC 2827[86] och RFC 3704[87].

Adressrymder som eventuellt kan filtreras kan vara bland annat så kallade bogon-prefix som är reserverade för privat bruk (RFC 6761[88]) eller för speciella ändamål och som inte är avsedda för öppen användning i internet. Andra motsvarande adressrymder kan vara nät som IANA eller lokala internetadressregister ännu inte har beviljat.[89]

Vid bogon-filtrering kan man använda BGP-routinginformation som tillförlitliga instanser tillhandahåller och där ändringar i bruket av adressrymderna centraliserat överförs i de regler som används för filtreringen. Utrustning som är försedd med default-bogon-listor ska inte användas, eftersom de är föråldrade.

I vissa exceptionella situationer kan teleföretaget komma överens med ett annat teleföretag om att en del av teleföretagets adressrymd tillfälligt routas så att trafiken kommer från det andra teleföretagets nät. Åtgärden ska planeras och genomföras noga och metoder som är lämpliga för samtrafiksituationen ska användas. Det teleföretag som förmedlar trafik är i första hand ansvarigt för att trafik som innehåller felaktiga källadresser inte förmedlas.

En situation där teleföretaget får ruttannonsering av ett annat teleföretag men inte annonserar den vidare anses inte vara en situation med felaktig källadress. Då motsvarar ruttannonseringen inte teleföretagets routinginformation, men samtrafiken mellan teleföretagen kan ändå förmedlas.

17.4 Filtrering av ruttannonseringar

Enligt föreskriften ska utgångspunkten vara att teleföretaget vid samtrafikgränssnitten från mottagen annonsering av rutter ignorerar sådana rutter som hör till teleföretagets egna adressblock eller till sådana adressblock som teleföretaget levererar till kunden och som inte kan förväntas bli annonserade av andra teleföretag. Föreskriften ger möjlighet att göra undantag från denna grundregel, om man särskilt har avtalat om det.

Teleföretaget ska förkasta sådana ruttannonseringar vars ROA-post (Route Origin Authorization) inte motsvarar de ROA-uppgifter som uppgetts i RPKI-databasen (Resource Public Key Infrastructure).

Inget teleföretag borde annonsera adressblock som ett annat teleföretag eller det andra teleföretagets kunder administrerar, eller mer precist rutter som innehåller block utan särskilt avtal. Till exempel vissa multihoming-lösningar kan förutsätta ett sådant avtal.

Obehörig annonsering kan vara avsiktlig eller oavsiktlig dirigering av trafiken till en utomstående aktörs system. Ett teleföretag som tar emot annonseringar av rutter ska för

[86] IETF RFC 2827, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, https://tools.ietf.org/html/rfc2827.
[87] IETF RFC 3704, Ingress Filtering for Multihomed Networks, https://tools.ietf.org/html/rfc3704.
[88] IETF RFC 6761, Special-Use Domain Names, https://tools.ietf.org/html/rfc6761.
[89] ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP), s. 11 (Bogon Filtering).

att skydda sig mot hot som obehörig annonsering kan förorsaka filtrera felaktig annonsering, t.ex. sådana adressblock som hör till andra teleföretag och deras kunder som nämnts ovan samt adressblock som inte borde förekomma i routing. Eventuella lösningsalternativ för filtreringen beskrivs i IETF:s definition RFC 7454[90].

Rekommendation

Transport- och kommunikationsverket rekommenderar att teleföretaget förverkligar den tekniska och operativa förmågan att filtrera BGP AS-vägar. Filtrering av vägar är en teknik som kan användas för att godkänna eller förkasta prefix, vars ursprung eller rutt kommer via ett visst AS. Denna teknik kan användas för att t.ex. förkasta prefix vars ursprung är ett privat AS om AS-systemet i fråga inte är kund hos teleföretaget. Mer information om filtrering av BGP AS-vägar finns i IETF:s definition RFC 7454[90].

17.5 Autentisering av ruttannonseringar

Föreskriften förutsätter att teleföretaget skapar ROA-poster för de domäner som det äger eller levererar till sina kunder. Dessutom ska företaget se till att posterna har undertecknats och publicerats i det relevanta internetadressregistret.

En faktor som avsevärt försämrar säkerheten i BGP är att äktheten hos ruttannonseringar vanligtvis inte kontrolleras på något sätt, eftersom man i regel litar på att den information om rutterna som man fått av det autonoma system som man utbyter rutter med stämmer. Vanligtvis är det så också, men det kan även finnas oavsiktliga eller avsiktliga fel i annonseringarna. För autentisering av routinginformation har det dock utvecklats lösningar, varav den kändaste och mest allmänt använda är RPKI. Med hjälp av RPKI är det möjligt för de autonoma systemen att verifiera de ruttannonseringar som de äger. Tekniskt sett sker detta genom att skapa ROA-poster, som bekräftas med en digital underskrift. ROA-posten anger vilket autonomt system som har auktoriserats att skapa och annonsera rutter till en viss grupp IP-adresser. För att ruttannonseringarna ska kunna verifieras ska routrarna konfigureras för att kontrollera routinginformationen genom att använda RKPI och vidta åtgärder för de rutter som inte klarar kontrollen. ROA-poster kan enklast skapas och undertecknas med hjälp av förtroendekedjor i lokala internetregister. För Finland är den regionala internetregistratorn RIPE NCC, på vars webbplats det finns heltäckande anvisningar för såväl skapande, hantering och undertecknande av ROA-poster som autentisering av ruttannonseringar med routrar[91].

Vid verifieringen av huruvida BGP-ruttannonseringarna är korrekta jämförs RPKI-information som validerats av de routrar som deltar i BGP-routingen med inkommande ruttannonseringar. Med validerad RPKI-information avses ROA-uppgifter från RPKI-validerade (RPKI Validator) servrar. RPKI-validerade servrar får informationen om ROA-posternas status från RPKI-databasen (RPKI Repository), som förvaltas av det regionala internetadressregistret.

I denna verifieringsprocess finns det tre möjliga slutresultat: "Valid", "Invalid" och "Not-Found".[92] Resultaten ”Valid” och ”Invalid” betyder att ROA-posten existerar och att den antingen motsvarar den RPKI-validerade ROA-posten i RPKI-databasen eller att dessa

[90] IETF RFC 7454, BGP Operations and Security: https://tools.ietf.org/html/rfc7454. Se även MANRS Action 1 och ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP).
[91] RIPE NCC, RPKI, https://www.ripe.net/manage-ips-and-asns/resource-management/rpki. Se även ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP), åtgärd 7.
[92] IETF RFC 6811, BGP Prefix Origin Validation, https://tools.ietf.org/html/rfc6811.

kriterier inte uppfylls. ”NotFound” betyder att ROA-posten antingen inte har skapats eller att den inte har publicerats i RPKI-databasen.

Från kraven på ROA-poster kan undantag göras för domäner som inte omfattas av systemet med register över internetadresser och domäner för vilka det är tekniskt omöjligt att skapa en ROA-post.

Utöver ovanstående åtgärder kan teleföretaget använda sig av till exempel BGPsec-tillägget i BGP-protokollet för att förbättra routingens säkerhet. IETF har beskrivit BGPsec-tillägget i RFC 8205[93] och RFC 8206[94]. Med hjälp av BGPsec kan man kryptografiskt säkerställa att varje AS längs nättrafikens rutt har auktoriserat ruttens annonsering till nästa AS.

18. Förhindrande av förfalskning av källadress i kundgränssnitt i IP-trafiken

I distribuerade överbelastningsangrepp använder man ofta förfalskade källadresser för kommunikationen för att göra det svårare att hitta den attackerande parten. Man kan förfalska källadressen till att tillhöra ett externt nät som inte har någonting att göra med attacken eller en slumpmässigt vald adress i målnätet. Förfalskade källadresser kan dessutom vara slumpmässigt valda från adressrymder som är reserverade för privat bruk eller för särskilda ändamål. Syftet med kraven på filtrering av IP-trafik som innehåller felaktiga källadresser är att begränsa problem som orsakas av attacker som begås med förfalskade käll-IP-adresser i nätet.

Som en lindrigare åtgärd än filtrering kan teleföretaget också kontakta kunden för att utreda situationen. Denna möjlighet bygger på att teleföretaget enligt lagen om tjänster inom elektronisk kommunikation kan hindra eller begränsa förmedling av meddelanden till kundens terminalutrustning för att förhindra hot och störningar mot informationssäkerheten i kommunikationsnät eller i tjänster som är anslutna till näten. En lindrigare åtgärd än begränsning är att teleföretaget kan identifiera en användare som orsakar hotet eller störningen och kontakta användaren eller den som representerar användaren för att eliminera hotet eller störningen.

18.1 Filtrering

För att blockera trafik som utnyttjar förfalskade källadresser ska ett teleföretag som tillhandahåller kundabonnemang filtrera sådan trafik från ett kundabonnemang till kommunikationsnätet vars källadress inte är anvisad kundabonnemanget i fråga. Teleföretaget ska vid behov kunna identifiera det kundabonnemang vars trafik mot nätet har förfalskade källadresser.

Filtreringen kan genomföras exempelvis så att källadressen för varje paket som tas emot i gränssnittet jämförs med en lista över godtagbara adressrymder och att varje paket vars källadress inte finns bland adressrymderna i listan blockeras.

För t.ex. ADSL-förbindelser kan filtreringen göras i koncentratorns DSLAM-nätelement, i termineringsutrustningen för DSL-nätets förbindelser eller i routern för stamnätet. Den ändamålsenliga punkten för filtreringen beror på nätutrustningarnas teknik, filtreringsförmågan och på de förfaringssätt som teleföretaget tillämpar vid filtreringen.

[93] IETF RFC 8205, BGPsec Protocol Specification, https://tools.ietf.org/html/rfc8205.
[94] IETF RFC 8206, BGPsec Considerations for Autonomous System (AS) Migration, https://tools.ietf.org/html/rfc8206.

18.2 Identifiering av användare

Teleföretaget ska av informationssäkerhetsskäl kunna identifiera en kundanslutning som har använt en viss IP-adress genom att behandla förmedlingsuppgifter som lagrats i en DHCP-logg. Det är nödvändigt att identifiera kundanslutningen för att informationssäkerhetsåtgärderna ska kunna riktas till rätt kundabonnemang, även om anslutningens IP-adress skulle ha ändrats.

Enligt Kommunikationsverkets tidigare tolkning (dnr 387/64/2009) får teleföretaget vid behov behandla förmedlingsuppgifter både i situationer som numera definieras i 272 § 1 mom. i lagen om tjänster inom elektronisk kommunikation och vid användning av sådana metoder som numera avses i paragrafens 2 mom. Enligt Kommunikationsverkets tolkning får teleföretaget behandla förmedlingsuppgifter förutom vid utförandet av en åtgärd som avses i 272 §, även vid förberedande åtgärder som är nödvändiga för att den egentliga åtgärden ska kunna utföras. En sådan förberedande åtgärd kan till exempel vara identifiering av en kund som använt en viss IP-adress genom behandling av identifieringsuppgifter som lagrats i en DHCP-logg.

19. Skydd av gränssnitt i mobilnätet

De nya användningsfallen i 5G-nät och de arkitekturlösningar som de kräver har introducerat nya gränssnitt i teleföretagens kommunikationsnät. Via dessa gränssnitt är det möjligt att överlåta även kontrollen av nätet till tredje parter, till exempel för partiell administration av en skiva eller en Edge Computing-enhet i kommunikationsnätet. De föregående nätgenerationernas signaleringsprotokoll används fortfarande i stor utsträckning och upprätthåller förbindelserna mellan olika nätgenerationer. Helhetsmässigt sett ökar detta hotytan, vars hantering kräver ett övergripande skydd av gränssnitten av teleföretagen genom att uppfylla skyldigheterna i denna föreskrift samt utifrån den egna hot- och riskbedömningen aktivt följa och genomföra rekommendationer som tagits fram av olika intressenter.

19.1 Signaleringsgränssnitt

Med signalering i mobilnät avses styrning av kontroll- och användarkommunikationen mellan olika element på önskat sätt. I takt med att näten utvecklas har mängden och behovet av signalering ökat. Kommunikationsnätet utökas med nya funktioner och mellan dem skapas nya signaleringsgränssnitt. Det gamla signalsystemet Signalling System 7 (SS7) användes redan i 2G- och 3G-näten. Det har använts exempelvis vid routing av samtal i teleföretag och från ett företag till ett annat, för utbyte av information om samtrafik eller för att informera abonnenter om vilka egenskaper som finns tillgängliga. I planeringen av SS7 beaktades en gång i tiden inte informationssäkerhetens betydelse tillräckligt, vilket har möjliggjort missbruk av SS7. En eventuell angripare kunde till exempel injicera SS7-trafik i ett mobilnät och ta emot information som angriparen inte borde få tillgång till eller olovligt övervaka nätets funktioner. Genom angrepp kan man även kartlägga mobilnätet med hjälp av olika skanningstekniker som används inne i nätet. Beroende på nätets struktur och angriparens läge kan angriparen kartlägga till exempel kärnnätet, radioaccessnätet eller IMS:s struktur.[95] Med hjälp av den information som samlats in i kartläggningen kan man inrikta angreppets följande fas och välja en lämplig metod för det.

I 4G-näten ersätter Diameter-protokollet SS7 som använts i 2G- och 3G-näten. På motsvarande sätt har Diameter i regel ersatts av HTTP/2 JSON i 5G-näten. Ett gemensamt

[95] Rao, S. P. – Chen, H. Y. – Aura, T., Threat modeling framework for mobile communication systems. Computers and Security 125 2023, 103047, s. 1–23.

drag för dessa protokoll är att eventuella angripare utnyttjar kärnnätets normala funktionalitet, exempelvis genom att utge sig för att vara ett HLR-/HSS-element i nätet, och genom ett angrepp kan man försöka ta reda på slutanvändarens position i nätet eller ta reda på nätets struktur. En annan typ av angrepp är överbelastningsangrepp i nätet med hjälp av vissa signaleringsmeddelanden. På detta sätt kan man förbruka nätresurser eller rikta angreppet direkt mot en viss användare. Detta borde beaktas i synnerhet i skyddet av olika typer av tillämpningsgränssnitt.

Enligt punkt 19.1.1 i föreskriften ska teleföretaget i sina gränssnitt i mobilnätet övervaka signaleringsgränssnittens informationssäkerhet samt planera, genomföra och upprätthålla åtgärder för att kunna hantera signaleringsgränssnittens informationssäkerhet. Hanteringsåtgärderna ska basera sig på vetskap om hot och riskbedömning.

Det är möjligt att förhindra eller lindra effekterna av angrepp mot signaleringsprotokoll exempelvis genom att filtrera signaleringsmeddelanden. Med en dedikerad signaleringsbrandvägg (Signalling Firewall, SigFW) som fungerar på kanten av nätet kan man filtrera signaleringsmeddelanden i applikationsskiktet redan innan de når det avsedda nätelementet och påverkar dess funktion. Även i nätelement som behandlar signalering (SS7 Signal Transfer Point, STP; Diameter Agents, DRA, DEA; 5G Security Edge Protection Proxy, SEPP) kan man beroende på tekniken utföra filtrering av trafiken på olika nivåer. Generellt kan man förbättra säkerheten genom att härda systemen, dvs. genom att ta onödiga funktioner i nätelementen ur bruk.

SEPP är en obligatorisk säkerhetsfunktion som definierats av 3GPP och som förbättrar säkerheten i trafiken mellan 5G-nät genom bl.a. autentisering, auktorisering och kryptering i N32-gränssnittet.[96] Genom att se till att SEPP-funktionaliteten är korrekt planerad, genomförd och underhållen kan man t.ex. dölja kommunikationsnätets arkitektur samt filtrera inkommande och utgående trafik. Dessutom kan man exempelvis sträva efter en så heltäckande kryptering som möjligt av de data som förmedlas för att säkerställa säkerheten för dataöverföringen i 5G-näten.

Rekommendationer

SS7-protokollet används fortfarande i stor utsträckning, vilket gör att det även i fortsättningen är motiverat att upprätthålla och utveckla säkerheten i det. Transport- och kommunikationsverket rekommenderar att den samnordiska SS7-rekommendationen, som upprättades år 2015, verkställs i så hög grad som möjligt för att man ska uppnå en heltäckande skydds- och observationsförmåga.[97]

För att säkerställa säkerheten för Diameter-protokollet rekommenderar Transport- och kommunikationsverket att man följer den rekommendation om Diameter-protokollet som GSMA har utarbetat och upprätthåller. Genomförande av åtgärderna i den hjälper teleföretag att skydda sig mot de flesta kända hot.[98]

19.2 Skivning av mobilnät

Med nätverksskivning avses logiskt åtskiljande av tjänsterna i t.ex. ett mobilnät för att man ska kunna tillhandahålla riktade tjänster som är optimerade för olika användningsfall. I takt med att 5G-näten utvecklas har följande användningsfall definierats:

[96] Cybersäkerhetscentret, 5G Security Architecture, s. 33–34 (på finska), https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/5g-security-architecture.
[97] Common Nordic Recommendations on SS7 Security Issues, 18.12.2015.
[98] GSMA, FS.19 – Diameter Interconnect Security.

- mobila bredbandstjänster (enhanced Mobile Broadband, eMBB), kommunikation mellan fordon (Vehicle to X, V2X)
- mycket pålitliga tjänster med låg latens (Ultra-Reliable Low Latency Communication, URLLC)
- storskalig kommunikation mellan IoT-enheter (massive Machine-Type Communication, mMTC)
- kommunikation mellan IoT-enheter med hög förmedlingsförmåga (High-Performance Machine-Type Communications, HMTC).

De rekommenderade egenskaperna hos ovanstående skivtyper och egenskaper beträffande tjänstens kvalitet har definierats i GSMA:s publikation.[99] De rekommenderade egenskaperna och värdena har härletts ur 3GPP:s tekniska definition[100] samt har från GSMA:s sida ansetts uppfylla minimikraven för de aktuella skivtyperna. När det är fråga om något annat än ovanstående användningsfall kan ett teleföretag som tillhandahåller en nätverksskiva mer fritt definiera egenskaperna tillsammans med kunden (Network Slice Customer, NSC). Det kan handla om t.ex. ett privat nätverk som genomförts med hjälp av en nätverksskiva (Public Network Integrated Non-Public Network, PNI-NPN).

Skydd av hanteringsförbindelser

Föreskriften förutsätter (punkt 19.2) att mobilnätets teleföretag skyddar nätverksskivans hanteringsförbindelse så att inga obehöriga kan skapa, ändra eller radera nätverksskivan och att inte skivans egenskaper eller uppgifter om abonnenterna eller användarna lämnas ut obehörigt. Målet med att skydda hanteringsförbindelsen är att hindra angripare från att obehörigt använda t.ex. avgiftsbelagda tjänster eller skapa en nätverksskiva som kan användas för att blockera tjänster eller följa kommunikationsnätets kunder. Angriparen kan också försöka genomföra till exempel ett man-in-the-middle-angrepp genom att ändra skivan för att omrouta trafiken.

I skyddet av en nätverksskivas hanteringsförbindelse är det skäl att beakta i synnerhet situationer där skivan har förverkligats som en tjänst (Network Slice as a Service, NSaaS) och kunden (NSC) har beviljats personliga åtkomsträttigheter till nätverkets funktioner och data. I sådana fall är det bra att noggrant definiera, begränsa och övervaka att kunden har åtkomst till endast i förväg överenskomna data. För att säkerställa informationssäkerheten kan man styra trafiken via en NEF-funktionalitet (Network Exposure Function), som till exempel kontrollerar utlämnande av information om egenskaperna hos 3GPP:s kärnnät utanför 3GPP-domänen samt verifierar och auktoriserar all meddelandetrafik som kommer utifrån.

Skivspecificerad bekräftelse av behörigheter

Föreskriften (punkt 19.1.3) förutsätter att teleföretaget riskbaserat utför skivspecificerad bekräftelse och auktorisering av behörigheterna (Network Slice Specific Authentication and Authorization, NSSAA) hos de terminalutrustningar som använder skivan. Utöver primär 3GPP-autentisering ska man vid skivspecificerad bekräftelse och auktorisering av behörigheter använda andra autentiseringsuppgifter än de som använts vid primär autentisering. Detta ska göras om det, med beaktande av informationssäkerhetshot och tekniska möjligheter avseende användning av skivan, är nödvändigt att bekräfta behörighet och genomföra autentisering.

Skivspecificerad bekräftelse och auktorisering av behörigheter mellan terminalutrustningen och en AAA-server (Authentication Authorization and Accounting Server) görs

[99] GSMA, Official Document NG.116 – Generic Network Slice Template.
[100] 3GPP TS 23.501.

med hjälp av en NSSAAF (NSSAAF Function) som fungerar som proxyserver. NSSAAF förmedlar information om nätverksskivan (Single-Network Slice Selection Assistance Information, S-NSSAI) och terminalutrustningens identifieringsuppgifter (Generic Public Subscription Identifier, GPSI) till AAA-servern. 3GPP-domänens identifierare ska inte lämnas ut till utomstående domäner.

3GPP Release 17 introducerar en ny funktion i åtkomsthanteringen av nätverksskivor (Network Slice Admission Control, NSACF) som möjliggör bättre hantering och användning av skivorna. Med hjälp av funktionen är det möjligt att övervaka och kontrollera den skivspecifika mängden registrerade terminalutrustningar och PDU-sessioner (Protocol Data Unit). Genom säkerhetsfunktionen är det möjligt att minska riskerna i synnerhet i situationer där hanteringsrätten för nätverksskivan ligger utanför 3GPP-domänen. För analys och vidarebehandling förmedlas de data som ska sändas till nätverksskivans innehavare (Application Function, AF) med hjälp av NEF-funktionaliteten.[101]

Föreskriften beaktar att det inte nödvändigtvis finns ett behov av särskild skivspecificerad bekräftelse och auktorisering av behörigheter i alla användningsfall, exempelvis om användningen av skivan inte är förknippad med några avvikande informationssäkerhetshot. Föreskriften beaktar på så vis även att den terminalutrustning som används kan begränsa möjligheterna att utföra ytterligare åtgärder, även om inga okontrollerade informationssäkerhetsrisker får uppkomma heller i sådana situationer.

Om ingen skivspecificerad auktorisering utförs är det möjligt att terminalutrustning som inte har behörighet till nätverksskivan använder dess resurser eller obehörigt får information om nätverkets egenskaper. Obehörig terminalutrustning kan vara vilken vanlig enhet som helst som kan ha lyckats göra en primär autentisering med hjälp av 3GPP-autentiseringsuppgifter, men som inte har de behörigheter som behövs för användning av en viss nätverksskiva.[102]

19.3 Edge Computing i kommunikationsnät

De nya användningsfallen i kommunikationsnät och i synnerhet mobilnät ställer krav på prestandan och tillförlitligheten, och för att möjliggöra dessa förs kommunikationsnätets system närmare slutanvändaren. Då kan användarens trafik styras längs en kortare rutt till tjänstens resurser eller så kan tjänsten till och med tillhandahållas lokalt inom ramarna för en Edge Computing-enhet. Karakteristiskt för en Edge Computing-miljö är att den består av flera olika aktörers program och utrustning samt gör det möjligt att utveckla nya, mångsidiga verksamhetssätt och tjänster för kunderna. Det är typiskt att den fysiska utrustningen, virtualiseringsplattformarna och applikationerna tillhandahålls av olika aktörer. Tillsammans med tredje parters applikationer samt olika virtualiseringslösningar bildar teleföretagets nätverksfunktioner en oenhetlig helhet som är mottaglig för sårbarheter, i synnerhet om man inte ägnar särskild uppmärksamhet åt saken. Därtill bör observeras att en Edge Computing-enhet på grund av sitt läge kan vara mer mottaglig för fysisk påverkan (angrepp) än de mest centraliserade funktionerna i teleföretagets nät.

I genomförandet och upprätthållandet av en Edge Computing-enhet är det skäl att i enlighet med tillverkarens anvisningar beakta härdning av de programkomponenter som förverkligas genom virtualisering, med beaktande av de risker som hänför sig till läget för de fysiska systemen i miljön. För att säkerställa säkerheten för Edge Computing-enheter och det övriga kommunikationsnätet ska förbindelsen mellan applikationerna,

[101] 3GPP, Network Slicing Security for 5G and 5G advanced systems, https://www.3gpp.org/technologies/slicing-security
[102] ENISA GL SO11, 5G Security Control Matrix: SO11-010.

NEF-funktionen och Edge Computing-miljön i sådana fall genomföras på ett säkert sätt genom ömsesidig, upprepad autentisering samt genom att säkerställa att NEF-funktionens säkerhetsfunktioner genomförs och upprätthålls under hela deras livscykel. Särskild uppmärksamhet ska ägnas åt arrangemang där styrningen av en Edge Computing-enhet utförs av en tredje part utanför 3GPP-systemet. För att garantera säkerheten i Edge Computing-enheten är det bra att genomföra säkerhetsåtgärder som är viktiga med tanke på nätverksskivningen och virtualiseringen, såsom nätverksspecifik åtkomst- och autentiseringshantering samt åtgärder för härdning av virtualiseringsmiljön och en övergripande hantering av sårbarheter.

Kapitel 4 Särskilda krav för internetaccesstjänster

20. Åtskiljande av trafik i internetaccesstjänster

Enligt punkt 20.1 i föreskriften ska teleföretag skilja kundabonnemangens trafik från varandra så att användarna av de olika kundabonnemangen inte obehörigt kan följa med varandras trafik. Teleföretaget ska säkerställa att det inte är möjligt att obehörigen omdirigera trafik mellan abonnemangen.

Internetanslutningar som nyttjar delad kapacitet bland abonnenterna har använts för exempelvis nät i husbolag. I dessa lösningar delas internetförbindelsen som dras till husbolaget mellan bolagets invånare med hjälp av husbolagets eller teleföretagets nätutrustningar. Motsvarande nätlösningar med delad kapacitet används i till exempel stadsnät där tjänsten är öppen för alla som befinner sig inom nätets räckvidd.

Det är möjligt att skilja abonnenternas trafik från varandra till exempel fysiskt med egna ledningar för trafiken eller logiskt med hjälp av anslutningsspecifika VLANs eller trafikkryptering. Abonnenternas trafik kan också skiljas åt med hjälp av portisoleringsegenskapen för DSLAM-koncentratorer eller switchar, i synnerhet då man använder en grupp-VLAN-identifierare.

Okrypterade WLAN-förbindelser används i synnerhet på ställen där det finns många rörliga abonnenter. Det är tekniskt möjligt att kryptera WLAN-förbindelser, men det skulle avsevärt försvåra tillhandahållandet av tjänsten, speciellt vad gäller hanteringen av krypteringsnycklar. Punkt 20.2 i föreskriften innehåller därför ett särskilt undantag som gör det möjligt att tillhandahålla okrypterade WLAN-förbindelser utan att åtskilja trafiken i radiogränssnittet. Om det är möjligt bör användarna informeras om riskerna med att använda okrypterade WLAN-förbindelser. Med WLAN-förbindelser avses förbindelser via trådlösa lokalnät i enlighet med IEEE-standard 802.11.[103]

21. Dirigering av e-posttrafik från konsumentabonnemang

Enligt punkt 21 i föreskriften ska teleföretaget förhindra obegränsad SMTP-trafik från konsumentabonnemang om det sker på andra sätt än via överenskomna servrar avsedda för den utgående SMTP-trafiken. Föreskriften gör det dock möjligt att göra undantag i begränsningen, varvid teleföretaget ska informera abonnenten om de risker som är förknippade med frågan, samt ha förmåga att reagera på eventuella störningssituationer i anslutning till frågan.

Obegränsad SMTP-trafik (port 25) från en anslutning till internet gör det möjligt för skadliga program att skicka skräppost. Genom att tillåta utgående e-posttrafik endast via servrar som teleföretaget tillhandahållit för utgående SMTP-trafik kan man effektivt

[103] IEEE, 802.11 standard, https://standards.ieee.org/ieee/802.11/7028/.

begränsa mängden skräppost som de skadliga programmen producerar. Begränsningen påverkar inte nämnvärt användarnas kommunikationsmöjligheter, då det är möjligt att skicka e-post även via postservern i det teleföretag som tillhandahåller internetaccess-tjänsten, med hjälp av autentiserad e-post[104] eller användargränssnitt för www-baserade e-posttjänster. Filtreringsåtgärden för port 25 begränsar dock genomförandet av e-postservrar i konsumentabonnemang.

Genom föreskriften bekräftas rekommenderad praxis för metoder för sändning av e-post som finns i IETF-dokument RFC 5068[105].

Genom föreskriften tillåts även vid behov obegränsad trafik. Med tillåten obegränsad SMTP-trafik avses möjlighet till trafik som går ut från nätverksrymd avsedd för teleföretagets konsumentabonnemang till mottagare utanför teleföretagets nät, genom kommunikationsport 25 som är reserverad för utgående SMTP-trafik.

Vissa konsumentkunder kan dock ha motiverat behov av direkt SMTP-trafik från sin konsumentanslutning vart som helst utanför teleföretagets nät. Ett sådant behov är bland annat då konsumentkunden administrerar över SMTP-trafiken på sin egen server. Föreskriften möjliggör avvikelse från filtrering i port 25 exempelvis för sådana här situationer. Beslutet om vilka undantag som görs överlåts åt teleföretaget, eftersom föreskriften inte innehåller någon skyldighet för teleföretag att göra kundspecifika undantag i filtreringen. Exempelvis tekniska begränsningar per abonnemangstyp kan begränsa genomförandet av sådana undantag.

Med förhindrande av obegränsad SMTP-trafik avses blockering av trafik som går ut från nätverksrymd avsedd för konsumentabonnemang till mottagare utanför teleföretagets nät, genom kommunikationsport 25 som är reserverad för utgående SMTP-trafik.

När obegränsad SMTP-trafik förhindras i enlighet med föreskriften får förhindrandet inte inverka på e-posttrafik som nyttjar andra kommunikationsportar, såsom e-postprotokoll som kräver användaridentifikation eller kryptering. Man ska i synnerhet se till att begränsningen inte gäller trafik till port 587 som används av Mail Submission-tjänsten som beskrivs i IETF-dokument RFC 6409[104]. Detta gör det möjligt för kunder till teleföretaget som tillhandahåller internetaccesstjänster att också tryggt och autentiserat kommunicera med e-postsystem som en annan e-posttjänsteleverantör förfogar över.

Enligt föreskriften kan teleföretaget undantagsvis tillåta obegränsad SMTP-trafik även på annat sätt än via överenskomna servrar avsedda för utgående SMTP-trafik. Då måste teleföretaget underrätta abonnenten om de risker som hänför sig till öppen trafik. Teleföretag ska även ha beredskap att snabbt reagera på störningar.

22. Skyldighet att filtrera skadlig trafik i internetaccesstjänster

Genom kraven i punkt 22 i föreskriften åläggs en skyldighet att filtrera skadlig trafik i internetaccesstjänster och upprätthålla dokumentation om de filtreringsåtgärder som används.

Föreskriften ålägger teleföretaget att ha tekniska färdigheter att temporärt filtrera skadlig trafik (se definitionen i punkt 2.3 i föreskriften). Syftet med föreskriften är därför att säkerställa att teleföretaget har färdiga och uppdaterade processer, handlingsmönster

[104] IETF RFC 6409, Message Submission for Mail, https://tools.ietf.org/html/rfc6409.
[105] IETF RFC 5068, Email Submission Operations: Access and Accountability Requirements, https://tools.ietf.org/html/rfc5068.

och system för att temporärt filtrera skadlig trafik så snabbt som möjligt. Tekniska färdigheter för filtrering omfattar naturligtvis förmågan att först upptäcka skadlig trafik och att sedan vid behov filtrera trafiken. Det är emellertid bra att observera att kravet i denna punkt också ingår i Transport- och kommunikationsverket föreskrift om störningar i televerksamheten, där 4 § innehåller bestämmelser om bland annat förmågan att upptäcka störningar i informationssäkerheten.

Genom att filtrera trafiken är det möjligt att exempelvis begränsa effekten av sådana överbelastningsangrepp där man använder specifik kontrolltrafik för att belasta system i nätet. Åtgärderna kan dessutom begränsa trafik som ett skadligt program orsakar mot en viss port.

Det bör observeras att filtreringsåtgärderna enligt 272 § 4 mom. i lagen om tjänster inom elektronisk kommunikation ska genomföras omsorgsfullt och att 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 de mål som har fastställts för åtgärderna. Åtgärderna ska avslutas om det inte längre finns förutsättningar enligt lagen att vidta dem.

Utöver den allmänna skyldigheten att ha filtreringsförmåga som åläggs i punkt 22 i föreskriften, innefattar punkt 26 i föreskriften särskilda krav på filtrering av skadlig e-posttrafik.

Skydd av teleföretagets system och tjänster mot överbelastningsangrepp behandlas även i punkt 6.3 i föreskriften.

22.1 Tekniska färdigheter att vidta filtreringsåtgärder

Teleföretaget ska utrusta sitt kommunikationsnät med ett system som möjliggör upptäckt av skadlig trafik. Vid behov ska systemet kunna kontrollera trafiken i kommunikationsnätet så noggrant att det möjliggör en ändamålsenlig provtagning.

På grund av den stora trafikvolymen i det allmänna kommunikationsnätet kan man i allmänhet inte ha ett sådant system utan att nätens prestanda avsevärt påverkas. Insamlingen av uppgifterna kan då basera sig på trafikprov, varvid man betraktar endast en del av de paket som förmedlas i nätet. Provtagningens noggrannhet ska vara sådan att den ger en tillräckligt exakt bild av trafiken i nätet.

Teleföretaget kan använda t.ex. ett automatiskt system för hantering av trafikvolymer eller exceptionella händelser i nätet som larmar om de förinställda gränsvärdena överskrids. För hantering av informationssäkerhetshändelser i nätet är det också möjligt att använda t.ex. automatiska system för upptäckt och förhindrande av intrång.

I en situation som äventyrar kommunikationsnätets eller -tjänstens informationssäkerhet kan teleföretaget bli tvunget att vidta tillfälliga åtgärder för att blockera trafik via en viss telekommunikationsport eller begränsa trafik till vissa mottagaradresser. Filtreringsåtgärderna ska avbrytas när hotet som orsakat fara för kommunikationsnätets eller -tjänstens informationssäkerhet är över.

Med tekniska färdigheter för filtrering avses exempelvis att teleföretagets nätelement stöder begränsning av trafikvolymer på basis av enskilda protokoll, adresser, portar och

nätaccesser. Begränsningar ska kunna genomföras så att nätets tillgänglighet inte äventyras i onödan. De tekniska färdigheterna förutsätter dessutom att teleföretagets nätoperatörscentral har förmåga att starta nödvändiga filtreringsåtgärder.

22.2 Filtreringsregler och dokumentation av dessa

Vid användning av olika filtreringslistor ska man ägna särskild uppmärksamhet åt att reglerna för filtrering hålls uppdaterade, så att föråldrade regler inte leder till en felaktig och onödig filtrering. Filtreringen får exempelvis inte begränsa ändamålsenlig användning av redan beviljade IP-nätresurser.

Uppdaterad dokumentation ska föras över tillämpliga filtreringsåtgärder, så att man har kännedom om filtreringar som är i användning i näten och tjänsterna samt så att man kan följa upp ändamålsenligheten med filtreringarna.

Filtrering kan göras i syfte att blockera skadlig e-posttrafik, på basis av ruttannonser för att hindra kapning av outnyttjade adressrymder eller t.ex. på basis av källadresser för att begränsa blockeringsattacker. Eftersom det i överbelastningsangrepp regelbundet också används rent förfalskade källadresser som dock routas, är det skäl att grundligt överväga behovet av adressfiltrering och se över uppdateringsmekanismerna.

23. Bortkoppling av internetaccesstjänster

När trafik som utgår eller kommer från ett kundabonnemang äventyrar informationssäkerheten i en kommunikationstjänst ska man ingripa i situationen först och främst genom de åtgärder som föreskrivs i punkt 22 i föreskriften, det vill säga genom filtrering av trafik i teleföretagets nät eller med andra lindrigare åtgärder än bortkoppling av kundabonnemanget, såsom genom att kontakta kunden. Om teleföretaget inte genom dessa åtgärder lyckas få kontroll över läget som äventyrar informationssäkerheten och som anknyter till kundabonnemanget, har teleföretaget rätt att vidta åtgärder för att eliminera hotet som den smittade terminalutrustningen orsakar.

Enligt Transport- och kommunikationsverkets vedertagna tolkning äventyrar smittad terminalutrustning, som är ansluten till teleföretagets nät och som exempelvis sänder stora mängder skräppost eller skadlig trafik, alltid informationssäkerheten i teleföretagets tjänster. Smittad terminalutrustning kan därmed utgöra en grund för att koppla bort anordningen från nätet med stöd av 273 § i lagen om tjänster inom elektronisk kommunikation.

Eftersom bortkoppling av abonnemanget gör att kunden inte kan använda abonnemanget i fråga, ska det finnas detaljerade planer och anvisningar för bortkopplingsprocessen. Dessutom ska processen genomföras så att driftsavbrottet eller användningsbegränsningarna är så korta som möjligt.

23.1 Bortkoppling

Att en tjänst i ett kundabonnemang kopplas bort från det allmänna kommunikationsnätet avser i denna föreskrift exempelvis tillfällig avstängning av de kommunikationsportar till vilka trafik från kundanslutningen sänds så att kommunikationstjänstens informationssäkerhet äventyras. På ett motsvarande sätt kan teleföretaget bli tvunget att begränsa trafiken för vissa applikationsprotokoll från kundanslutningen om trafiken äventyrar kommunikationsnätets informationssäkerhet. Med orsaker som beror på kundanslutningen avses generellt inte att en kundanslutning eller en www-tjänst som kopplats

till nätet via kundanslutningen t.ex. är mål för ett överbelastningsangrepp och därför tar emot exceptionellt stora trafikvolymer i en viss situation.

Vid ombesörjandet av informationssäkerheten och i bortkopplingssituationer är det skäl att ägna uppmärksamhet åt att förmedlingsuppgifter får behandlas endast då det är frågan om hot mot eller kränkningar av informationssäkerheten i kommunikationsnät och -tjänster. Teleföretaget har således inte rätt att behandla förmedlingsuppgifter till exempel för att hindra användningen av abonnemanget vid brott som inte äventyrar tjänstens informationssäkerhet. Ett undantag är dock förberedelse till betalningsmedelsbedrägerier som avses i 272 § 1 mom. 3 punkten i lagen om tjänster inom elektronisk kommunikation (se även kapitel 4 i motiveringspromemorian).

23.2 Bortkopplingsprocess

Om möjligt ska kunden kontaktas, till exempel per telefon eller e-post, innan systemet kopplas bort från det allmänna kommunikationsnätet. Att kunden hörs får dock inte onödigt äventyra ombesörjandet av tjänstens informationssäkerhet.

Åtgärderna för bortkoppling ska göras enligt de processer som teleföretaget i förväg har specificerat. De vidtagna åtgärderna och i synnerhet orsaken till bortkopplingen ska registreras för eventuell senare utredning.

Anvisningarna för bortkopplingen ska innehålla nödvändiga förfaringssätt för att återkoppla kundanslutningen till kommunikationsnätet, när teleföretaget har konstaterat att informationssäkerhetshotet mot kommunikationstjänsten är över. När det gäller skadlig trafik som ett skadligt program orsakar kan anslutningen återinkopplas till kommunikationsnätet efter att kunden har kontaktat teleföretaget och meddelat att han eller hon har tagit bort det skadliga programmet från sitt system.

Då tjänste- och nätverksoperatörerna är olika aktörer, kommer de sinsemellan överens om principerna för det praktiska genomförandet av bortkoppling. Båda parterna ska ha möjlighet att vidta behövliga åtgärder för att sörja för informationssäkerheten i sin tjänst eller sitt nät. Den andra parten ska underrättas om bort- och återinkopplingen utan dröjsmål.

I samband med åtgärderna kan speciella förhållanden som beror på anslutningstypen beaktas. Om det t.ex. finns ett informationssäkerhetsproblem i mobilabonnemangets mobildatatjänst kan teleföretaget endast hindra användningen av mobildatatjänsten tills informationssäkerhetsproblemet är utrett.

Om kundabonnemangen omfattas av s.k. automatisk kontroll, sker bortkopplingen av kundabonnemangen eller vissa tjänster i kundabonnemanget normalt automatiskt utan manuella åtgärder från operatörens sida, för t.ex. 30 minuter, när gränsvärdena för skadlig trafik har överskridits. När abonnemanget är bortkopplat kan kundens trafik styras till en tjänst där kunden underrättas om orsaken till bortkopplingen och om eventuella åtgärder som kunden kan vidta för att avhjälpa felet. Dessutom kan kunden ha möjlighet att besöka behövliga webbplatser för att till exempel installera virusskydd och uppdatera operativsystemets programvara. Detta förfarande minskar behovet av en mer varaktig bortkoppling.

Vid användning av automatiska system för stängning och öppnande av kundabonnemang i syfte att sörja för informationssäkerheten i tjänsten, ska kunden underrättas om de principer som hänför sig till den tillfälliga stängningen och öppnandet av abonnemanget.

Kapitel 5 Särskilda krav på tjänster för text- och multimediemeddelanden

24. Filtrering av text- och multimediemeddelandetrafik

Föreskriften (punkt 24) förutsätter att teleföretaget har ändamålsenliga system och förfaringssätt för filtrering av text- och multimediemeddelandetrafik som identifierats som skadlig. Med detta avses såväl teknisk beredskap som i förväg definierade processer och anvisningar. Teleföretag ska ha förmåga att filtrera skadliga meddelanden i både den inkommande och den utgående SMS-trafiken. Underpunkterna 1 och 2 om filtreringsskyldigheten motsvarar för övrigt underpunkterna 1 och 2 i punkt 26 om filtrering av e-post, men beträffande SMS- och MMS-meddelanden har det inte identifierats något särskilt behov av att föreskriva om den filtrering som görs för att säkerställa funktionen hos de system som hänför sig till produktionen av tjänsten.

Genom filtrering som baserar sig på uppgifter om avsändare och andra förmedlingsuppgifter i text- eller multimediemeddelanden samt meddelandenas innehåll kan man ingripa i synnerhet i situationer där någon med hjälp av text- eller multimediemeddelanden försöker genomföra en storskalig kampanj för utskick av skadliga program eller nätfiskemeddelanden.

Identifieringen av skadlig trafik kan basera sig exempelvis på information om hot som meddelats av Cybersäkerhetscentret vid Transport- och kommunikationsverket eller andra teleföretag, på meddelanden från teleföretagets kunder eller på information från andra aktörer som bedömts vara tillförlitlig.

Som en lindrigare metod för att filtrera meddelanden möjliggör föreskriften utmärkning av meddelanden som misstänks vara skadliga med en identifierare (t.ex. genom att ändra sender ID:t eller lägga till text i början av meddelandet) eller, när det är tekniskt sett möjligt, förhindrande av funktionen hos länkar i meddelanden. Ovanstående åtgärder hindrar att mottagaren vilseleds utan att helt och hållet förhindra att meddelandena levereras t.ex. i situationer där man vid åtgärdsögonblicket inte med tillräckligt stor säkerhet har kunnat fastställa att ett meddelande är skadligt. Åtgärderna ska i så liten grad som möjligt inverka på förmedlingen av sakliga meddelanden.

Beträffande SMS-tjänster kan en SMS-brandvägg användas för filtreringen. Beträffande MMS-tjänster är inga lika etablerade tekniska lösningar nödvändigtvis lättillgängliga. Utvecklingen av nya tekniska lösningar är inte nödvändigtvis heller motiverat i förhållande till hotet, när man beaktar den relativt låga användningen av tjänsten. Därför innehåller punkt 24.3 i föreskriften ett undantag enligt vilket man beträffande MMS-tjänster under vissa förutsättningar kan låta bli att filtrera meddelanden baserat på innehåll och förmedlingsuppgifter. I sådana fall förutsätts att teleföretaget på andra sätt ska upptäcka störningar i informationssäkerheten och snabbt kunna reagera på dem. En observation kan inkludera exempelvis observation av avvikande mängder meddelanden, vilket kan tyda på att terminalutrustningen är infekterad. Istället för genom filtrering kan teleföretaget i sådana fall reagera på ett så lindrigt sätt som möjligt som lämpar sig för att eliminera konsekvenserna av informationssäkerhetsstörningen. Ett sådant sätt kan vara att t.ex. förhindra sändning av MMS-meddelanden tills det skadliga programmet har raderats från terminalutrustningen. Åtgärderna ska vara i linje med 272 § i lagen om tjänster inom elektronisk kommunikation.

Kapitel 6 Särskilda krav för e-posttjänster

Detta kapitel behandlar de skyldigheter som fastställs i föreskriftens kapitel 6.

25. Kontaktuppgifter för e-posttjänster och administrering av adressresurser

Föreskriften förutsätter att teleföretaget ska ha postmaster- och abuse-e-postadresser eller abuse-kontaktuppgifter för de domännamn som används för tillhandahållande av e-posttjänster. Meddelanden som kommer till dessa adresser ska kontrolleras regelbundet. Med kravet sörjer man för att det finns tillgång till en kontaktpunkt för information om eventuella störningar i verksamheten eller användningen, oberoende var meddelaren befinner sig.

Föreskriften förutsätter också att en e-postadress som blir ledig får överlåtas till en annan kund först då sex månader har gått efter det att e-postadressen blev ledig. Meddelanden sänds ofta till en e-postadress även efter det att adressen har stängts. Om en adress som blivit ledig genast eller snart efter att den stängts gavs till en annan kund, skulle den nya kunden kunna börja få e-postmeddelanden avsedda för den tidigare användaren. För att förhindra missbruk av e-postmeddelandens konfidentialitet och e-postadresser ska en e-postadress som blivit ledig hållas i karantän i sex månader innan den på nytt kan frigöras för användning.

25.1 Kontaktuppgifter för teleföretag som tillhandahåller e-posttjänster

Teleföretag som tillhandahåller e-posttjänster ska se till att företaget har postmaster- och abuse-e-postadresser eller abuse-kontaktuppgifter för de domännamn som används för tillhandahållande av e-posttjänster. Meddelanden som kommer till dessa adresser ska kontrolleras regelbundet.

Postmaster- och abuse-adresserna har stor spridning och samlar ofta obefogad kommunikation. Därför bör teleföretaget ombesörja uppföljningen av adressen så att behandlingen av sakliga meddelanden inte fördröjs på grund av den stora mängden skadlig e-posttrafik. Om teleföretaget har ett stort antal domännamn, är det skäl att dirigera inkommande e-postmeddelanden till domännamnens postmaster- och abuse-adresser till tillämpliga kontaktpunkter.

Teleföretaget kan också överlåta uppföljningen av kontakterna till en part som ansvarar för domännamnet. Det är m.a.o. också möjligt att agera på så sätt att den instans som ansvarar för domännamnet följer upp meddelanden till postmaster- och abuse-adresser på teleföretagets vägnar.

25.2 Återanvändning av e-postadresser som blivit lediga

Teleföretag som tillhandahåller e-posttjänster får överlåta en e-postadress, som blir ledig, till en annan kund först då sex månader har gått efter det att e-postadressen blev ledig. Om den tidigare innehavaren av en e-postadress önskar tillbaka sin gamla e-postadress inom sex månader efter att adressen blev ledig, kan adressen överlåtas till honom eller henne. Rätten att få tillbaka en e-postadress förpliktar emellertid inte i sig tjänsteleverantören att spara e-postmeddelanden på e-postkontot efter det att kontot har avslutats. En sådan skyldighet kan dock basera sig på t.ex. en överenskommelse mellan parterna.

26. Särskild skyldighet att filtrera e-posttjänster

Denna punkt i föreskriften behandlar förmågan att identifiera skadlig e-posttrafik. Dessutom fastställs kraven på filtrering av e-posttrafik.

En stor del av e-posttrafiken kan i dag tolkas som skadlig trafik. E-postmeddelanden som identifieras och filtreras så tidigt som möjligt minskar belastningen i e-postsystemet och förmedlingen av sakliga meddelanden blir bättre.

Syftet med kraven är att minska på skadlig e-posttrafik och mängden skräppost via servrarna i teleföretag som tillhandahåller e-posttjänster. Detta minskar belastningen i e-postsystemet, förebygger skadlig inverkan på systemet (t.ex. vid överbelastningsangrepp), förbättrar ryktet för teleföretagets e-postservrar och säkerställer att sakliga meddelanden går fram. Genom att filtrera t.ex. skadliga inkommande e-postmeddelanden förhindras att innehåll som är skadligt för kundens informationssäkerhet och kommunikationsnäten hamnar i kundens e-postlåda och för behandling. Det är också enklare för kunden att behandla sina e-postmeddelanden då sakliga meddelanden inte behöver urskiljas från skadliga meddelanden. Samtidigt blir den av kunderna upplevda servicekvaliteten och tillgängligheten bättre.

Det finns flera olika metoder för identifiering och behandling av skadlig e-posttrafik. Föreskriften förutsätter inte användning av några särskilda metoder, utan teleföretaget som tillhandahåller e-posttjänster har möjlighet att välja de metoder som lämpar sig bäst för den erbjudna tjänsten.

Eftersom en del användare av e-posttjänster själva vill försäkra sig om att ingen felaktig filtrering görs, har e-posttjänsteleverantörerna även möjlighet att märka ut sådan trafik som upptäckts vara skadlig i stället för att filtrera den. Föreskriften möjliggör även kundspecifika överenskommelser om att e-posttjänsteleverantören låter bli att filtrera eller märka ut den inkommande trafiken.

26.1 Identifiering av skadlig e-posttrafik

Identifiering av skadlig e-posttrafik är en förutsättning för alla behandlingsåtgärder som leverantören av e-posttjänster gör, t.ex. för filtrerings- och märkningsåtgärder. Ett teleföretag som tillhandahåller e-posttjänster ska ha aktuella och tillförlitliga mekanismer för att identifiera skadlig eposttrafik.

Identifiering av skadlig e-posttrafik och den filtrering eller märkning som görs på basis av identifieringen kan basera sig på skadliga e-postkällors identifieringsmekanismer, heuristiska filtreringssystem, virusfiltrering av utgående trafik, avvikande mängd e-posttrafik från en kund eller till exempel på kontroll av om meddelandets rubrikuppgifter överensstämmer med internetstandarder. Olika tillgängliga identifieringsmekanismer beskrivs i kapitel 2 i bilagan till denna motiveringspromemoria.

På basis av e-posttrafikkällorna kan en stor del av de kända behöriga källorna för e-postmeddelanden samt kända källorna för skadliga e-postmeddelanden identifieras. Identifieringen kan göras till exempel på basis av avsändarens webbadress, domännamn eller e-postserver. Huruvida meddelandet är skadligt avgörs på basis av uppgifter som man fått eller insamlat på förhand om meddelanden som skickats via källan eller på analys av meddelandets innehåll. Genom att identifiera behöriga källor är det möjligt att undvika filtrering av relevant e-posttrafik som kan bero på felaktig identifiering. Genom att identifiera källorna för skadlig e-posttrafik är det i sin tur möjligt att hindra leverans av meddelanden från dessa källor till e-postlådor eller att märka ut e-postmeddelanden som tvivelaktiga innan man levererar dem till kundens e-postlåda.

En leverantör av e-posttjänster kan dock upptäcka endast en del av den skadliga e-posttrafiken på basis av e-postkällorna. Därför ska leverantören också ha andra metoder

för att upptäcka skadlig e-posttrafik. Flera av dessa metoder kan dock medföra avsevärda kostnader för e-posttjänsteleverantören. Snävare identifieringskriterier är också mer utsatta för felaktiga tolkningar. Ett teleföretag som tillhandahåller e-posttjänster kan bland flera alternativ välja de mekanismer som det använder i sitt system så att en betydande del av den skadliga e-posttrafiken blir identifierad och i så liten utsträckning som möjligt äventyrar förmedlingen av sakliga meddelanden.

Det är möjligt att identifiera en betydande del av den skadliga eposttrafiken bara genom att använda en enda metod. Om man vid identifiering av skadlig trafik samtidigt använder flera metoder som kompletterar varandra förbättras resultaten emellertid ofta. Varje metod har sina fördelar jämfört med andra metoder, men tyvärr finns det också problem med varje metod. Leverantören av e-posttjänster ska vara medveten om för- och nackdelarna med de metoder leverantören använder och bedöma effekterna av dessa innan metoderna tas i bruk.

Förutom de för alla kunder tillgängliga grundläggande identifieringsmekanismer som uppfyller kriterierna ovan, kan en leverantör av e-posttjänster tillhandahålla sina kunder även mer avancerade och mer skräddarsydda mekanismer för identifiering och behandling av skadlig trafik, till exempel genom ett separat avtal.

26.2 Rekommendationer om identifiering av skadlig e-posttrafik

Det rekommenderas att teleföretag som tillhandahåller e-posttjänster gör en kontroll för att identifiera skadlig e-posttrafik redan vid SMTP-kontakten. På så vis är det möjligt att spärra en stor del av den skadliga e-posttrafiken redan innan den kommer in i e-postsystemet. Åtgärden minskar betydligt den skadliga e-posttrafikens belastning på e-postservrarna.

Vid identifiering av skadlig e-posttrafik rekommenderas det att flera metoder används samtidigt. Precisionen för identifieringen av skadlig e-posttrafik förbättras och sålunda används t.ex. också snävare kriterier för identifiering.

Användning av accesslistor rekommenderas för att förhindra felaktig tolkning i situationer då e-posttjänsteleverantören använder spärr- och filtreringsmetoder.

26.3 Behandling av inkommande e-posttrafik

Med behandling av inkommande e-posttrafik avses åtgärder som kan vidtas för e-postmeddelanden som kommer till kunderna via e-posttjänsteleverantörens mottagningsservrar (MDA) eller proxyservrar. Åtgärderna omfattar identifiering av källorna för skadlig e-posttrafik, identifiering av skadlig e-posttrafik, filtrerings- och utmärkningsåtgärder för trafik som identifierats som skadlig samt leverans av trafik till kunden.

Med filtrering av inkommande e-posttrafik avses förhindrande av att e-posttrafik som identifierats som skadlig hamnar i kundernas e-postlåda. Genom att filtrera skadliga e-postmeddelanden kan man minska belastningen i e-postservrarna och mängden skadliga e-postmeddelanden som hamnar i kundernas e-postlåda. På så sätt blir det också enklare att gå igenom sakliga meddelanden. Samtidigt förebygger man de skadliga e-postmeddelandenas verkningar exempelvis när kunderna öppnar e-postbilagor eller styrs till en webbplats med skadligt program via en länk i ett e-postmeddelande. Med filtrering av e-posttrafik kan man förbättra den av kunderna upplevda servicekvaliteten och tjänstens informationssäkerhet.

Enligt föreskriften ska en e-posttjänsteleverantör från inkommande e-posttrafik märka ut eller filtrera sådan e-posttrafik som leverantören på basis av identifieringsmekanismer för skadlig e-posttrafik eller dess källor har bedömt som skadlig. I stället för automatisk filtrering av trafik som har identifierats som skadlig kan e-posttjänsteleverantören också t.ex. dirigera en del eller alla meddelanden som leverantören har upptäckt att är skadliga och har märkt ut till en separat användarspecifik mapp avsedd för skadlig e-post, där en viss mängd meddelanden eller meddelanden under en viss tid kan sparas och kontrolleras av användaren. E-posttjänsteleverantören kan också avlägsna det innehåll från meddelandena som identifierats som skadligt, innan meddelandet levereras till kunden.

Tjänsteleverantören kan särskilt komma överens om att trafik som identifierats som skadlig inte filtreras eller märks ut som skadlig. E-posttjänsteleverantören kan således inte som standard genomföra tjänsten utan filtrering eller utmärkning av trafik som identifierats som skadlig, och därför kan detta alternativ inte inkluderas som standard i standardavtal.

Trots ovan nämnda undantag ska e-posttjänsteleverantören ändå alltid filtrera sådan e-posttrafik som identifierats som skadlig som äventyrar informationssäkerheten (inklusive tillgängligheten) i de system som används för att producera e-posttjänsten.

26.4 Behandling av utgående e-posttrafik

Med behandling av utgående e-posttrafik avses åtgärder som kan vidtas för e-postmeddelanden som förmedlas via en e-postserver för utgående trafik (MSA). Åtgärderna omfattar identifiering av behöriga avsändare samt filtrering av utgående e-posttrafik som identifierats som skadlig via en e-postserver för utgående trafik.

Enligt föreskriften ska ett teleföretag som tillhandahåller e-posttjänster filtrera sådan utgående e-posttrafik som identifierats som skadlig. För att genomföra detta kan teleföretaget bland flera alternativ välja de mekanismer som används i systemet (se t.ex. kapitel 2 i bilagan till denna motiveringspromemoria). Målet är att en betydande del av den skadliga utgående e-posttrafiken blir identifierad och filtrerad, dock så att förutsättningen för att sakliga meddelanden ska gå igenom äventyras så lite som möjligt.

Om en e-posttjänsteleverantör märker att en kunds terminalutrustning används för förmedling av skadlig e-posttrafik ska e-posttjänsteleverantören filtrera den skadliga e-posttrafik som sänds från kunden eller spärra kundens e-posttrafik och om det är möjligt kontakta kunden.

27. Öppna proxyservrar för e-post

Öppna proxyservrar för e-post (se definitionen i punkt 2.2) används allmänt för förmedling av skadlig e-posttrafik.

Genom att identifiera öppna proxyservrar för e-post och hindra användning av tredje parters e-postservrar för förmedling av e-postmeddelanden kan mängden förmedlad skadlig e-posttrafik minskas.

Teleföretag som tillhandahåller en e-posttjänst ska se till att de e-postsystem som företaget administrerar inte fungerar som öppna proxyservrar. De testningsåtgärder som utförs, samt omsorgsfull definition av inställningar, är exempel på hur man sörjer för e-postsystemens driftsäkerhet i samband med ibruktagande och ändringar av system och tjänster.

Teleföretag ska regelbundet testa alla de e-postsystem som det administrerar för att försäkra sig om att systemen inte fungerar som öppna proxyservrar för e-post. Om ett företag inte har skaffat ett eget system för testning kan det använda de offentliga tjänster som är allmänt tillgängliga på internet för testningen.

För sådana e-postservrar för utgående trafik som hör till internetanslutningen avses med denna skyldighet att det är möjligt att skicka e-post utan identifiering endast från det aktuella teleföretagets eget nät.

28. Förbindelse mellan kund och e-postserver

Med förbindelse mellan kund och e-postserver avses en förbindelse mellan kunden (MUA, Mail User Agent) och e-postlådan (MS) samt mellan kunden (MUA) och e-postservern för utgående trafik (MSA).

Med skyddad förbindelse mellan kund och e-postserver samt mellan kund och e-postlåda avses identifiering av kunden och kryptering av trafiken mellan kunden och tjänsten.

Användarnamn och lösenord förmedlas mellan kunden och e-postservern. Genom att skydda förbindelserna mellan kunden och servern är det möjligt att förhindra att denna information hamnar hos tredje part samt förhindra missbruk av servern och förbättra tjänstens informationssäkerhet. Genom att skydda förbindelsen mellan kund och server kan man också säkerställa att kundernas meddelanden i trafiken mellan kunden och servern förblir konfidentiella. Genom att skydda förbindelsen kan man dessutom erbjuda kunderna ett tryggt sätt att använda e-posttjänsten oberoende av accessnät och öka kundernas förtroende för tjänsten.

Det är emellertid skäl att informera kunderna om att en skyddad förbindelse mellan kunden och servern inte nödvändigtvis innebär att förbindelsen är skyddad från den ena ändan till den andra, från avsändaren till mottagaren.

På grund av det sätt på vilket webbläsarbaserade e-posttjänster (webmail) normalt används är det befogat att förbindelserna alltid är skyddade.

Leverantörer av e-posttjänster ska som primärt alternativ erbjuda kunderna en skyddad förbindelse mellan kunden och e-postlådan samt mellan kunden och e-postservern för utgående trafik. Skyldigheten gäller också andra än webbläsarbaserade e-posttjänster.

Denna skyldighet avser att ett teleföretag ska erbjuda användarna av e-posttjänsten tillgång till skyddade förbindelser och att i de anvisningar för användning som distribueras till kunderna och som kunderna har tillgång till ska användning av skyddade förbindelser anvisas kunderna antingen som det primära eller enda alternativet.

Rekommendationen är att ett SMTP-AUTH-protokoll används för att identifiera behöriga användare och öppna en skyddad kundförbindelse från kunden till en proxyserver för e-post.[106] För detta ändamål kan t.ex. IMAP- eller POP-förbindelser skyddade av SSL/TLS-protokoll användas mellan kunden och e-postlådeservern.[107]

[106] IETF RFC 4954, SMTP Service Extension for Authentication, https://tools.ietf.org/html/rfc4954.
[107] IETF RFC 2595, Using TLS with IMAP, POP3 and ACAP, https://tools.ietf.org/html/rfc2595 och IETF RFC 4616, The PLAIN Simple Authentication and Security Layer (SASL) Mechanism, https://tools.ietf.org/html/rfc4616.

Vid användning av port 25 för sändning eller förmedling av e-post (reläande) kan man för skydd av förbindelsen även använda STARTTLS även när användaren inte autentiseras.[108]

De webbläsarbaserade e-posttjänsternas kundförbindelser ska alltid vara skyddade. Den rekommenderade skyddsmetoden för transportskiktet är TLS-protokoll.[109]

Kapitel 7 Ikraftträdandebestämmelser

Detta kapitel behandlar föreskriftens kapitel 7, det vill säga föreskriftens bestämmelser om ikraftträdande och övergångstid.

29. Ikraftträdande [och övergångstid]

[Denna föreskrift träder i kraft tre månader efter att föreskriften utfärdats.]

[108] IETF RFC 3207, SMTP Service Extension for Secure SMTP over Transport Layer Security, https://tools.ietf.org/html/rfc3207 och IETF RFC 7817, Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols, https://tools.ietf.org/html/rfc7817.
[109] Vid användning av HTTPS-protokollet se IETF RFC 2818, HTTP Over TLS, https://tools.ietf.org/html/rfc2818.

BILAGA Övriga frågor som har samband med föreskriftens ämnesområde

Denna avdelning innehåller rekommendationer om televerksamhetens informationssäkerhet, Transport- och kommunikationsverkets tolkningar samt annat material som bakgrund för den ämneshelhet som föreskriften omfattar.

1. Vilseledande e-postadresser

Vilseledande e-postadresser skapas för att leda en annan part att tro att innehavaren av adressen är en annan person eller aktör. Med vilseledande e-postadress avses exempelvis en e-postadress som är registrerad i en annan persons eller ett annat företags namn, ett företags FO-nummer eller vissa allmänt kända adresser (såsom postmaster, webmaster eller kundtjänst).

Om ett teleföretag som tillhandahåller e-posttjänster upptäcker eller informeras om en vilseledande e-postadress som registrerats på företagets domännamn ska teleföretaget ingripa. Teleföretaget har rätt att ta ur bruk adresser som har skapats i avsikt att vilseleda.

E-postadressen kan också bestå av någon annans personuppgifter. Enligt personuppgiftslagen gäller för personuppgifter felfrihetskravet och därtill hörande skyldighet att rätta till personuppgifter. Det kan också vara kriminalrättsligt straffbart att använda någon annans personuppgifter i vinningssyfte.

Transport- och kommunikationsverket rekommenderar att de teleföretag som tillhandahåller e-posttjänster inte beviljar sina kunder sådana vilseledande e-postadresser eller deras motsvarigheter på finska som definieras i RFC 2142[110] och hänför sig till företagets eget domännamn.

2. Mekanismer för att identifiera skadlig e-posttrafik

I detta kapitel presenteras olika kända och allmänt använda mekanismer för identifiering av skadlig e-posttrafik.

2.1 Spärrlistning

Kontakter och e-postmeddelanden från kända, obehöriga e-postkällor kan identifieras och filtreras med hjälp av spärrlistor (block list). En spärrlista består av webbadresser som i regel fungerar som källor till skadlig e-posttrafik.

Listan kan också bestå av enskilda e-postadresser, domännamn eller e-postservrar som använts för att skicka skräppost. Spärrlistan kan upprätthållas av e-posttjänsteleverantören eller tredje part, eller vara användarens personliga lista. E-postsystem använder normalt centraliserade spärrlistor som en tredje part upprätthåller.

Då man använder och väljer spärrlistor ska man vara extra noggrann för att undvika felaktiga tolkningar. Statiska spärrlistor är ofta otillförlitliga, eftersom källorna till skadlig e-posttrafik ofta ändras och en eventuell statisk felaktig information på spärrlistan

[110] IETF RFC 2142, Mailbox names for Common Services, Roles and Functions, https://tools.ietf.org/html/rfc2142.

hindrar saklig e-posttrafik för en lång tid. Radering av information från en statisk spärrlista kräver alltid manuellt arbete. Spärrlistor som upprätthålls dynamiskt däremot uppdateras snabbt och felaktiga uppgifter raderas regelbundet från listorna.

Eftersom informationen på en spärrlista kontinuerligt ändrar, är det i allmänhet inte värt att göra upp någon egen lista. För att e-posttjänstens tillgänglighet ska kunna säkerställas är det, när spärrlistor används, skäl att undvika sådana spärrlistor som enskilda användare har gjort upp över vissa stora domäner. Dessutom ska man undvika sådana spärrlistor där orsakerna till att någon hamnar på listan är oklara, det inte finns något klart förfarande för hur man kommer bort från listan eller användning av listan inte rekommenderas för stora tjänsteleverantörer.

Vid val av en spärrlista som upprätthålls av tredje part ska e-posttjänsteleverantören ägna särskild uppmärksamhet åt följande egenskaper hos listan:

- Principerna för listning publiceras
- Det är enkelt att ta bort information från listan och det finns anvisningar för det
- Kontaktuppgifterna för upprätthållaren av listan är offentliga
- Listan baserar sig inte på ett enskilt felaktigt meddelande
- Listan uppdateras regelbundet

När man använder spärrlistor ska man observera att listorna kan innehålla felaktig information och att användningen av listan därför kan hindra saklig e-posttrafik. En lista som upprätthålls av tredje part ska följas kontinuerligt. Olika listor innehåller i allmänhet olika källor, och därför ger användning av flera listor samtidigt ofta det bästa resultatet. När de olika listorna identifierar källor som skiljer sig från varandra ökar procentandelen identifierad skadlig trafik som kommer till e-postservern från olika källor. Vid heuristisk filtrering kan spärrlistor också användas som en del av bedömningen av en e-postkällas skadlighet. I sådana fall leder en enskild felaktig listning inte till att ett sakligt meddelande filtreras.

En e-posttjänsteleverantör som använder spärrlistor ska till sitt förfogande ha en fungerande mekanism för identifiering av de kända, viktigaste och sakliga e-postkällorna. När föreskriften publiceras avses med detta användning av frilistor. För att minimera eventuella felaktigheter i listan ska e-posttjänsteleverantören göra upp en lista (frilista) över väsentliga samarbetspartner och pålitliga inhemska tjänsteleverantörer som passerar e-postsystemets adresser på spärrlistan.

2.2 Frilistning

På en frilista (allow list) antecknas att mottagandet av meddelanden är tillåtet via vissa webbadresser, e-postservrar eller e-postadresser som är allmänt kända som pålitliga avsändare av sakliga meddelanden. Pålitliga avsändare kan exempelvis vara kända e-posttjänsteleverantörer och samarbetspartner.

Användningen av en frilista är i praktiken nödvändig då andra spärr- eller filtreringsmetoder som baserar sig på en e-postkälla används. Med hjälp av frilistan kan man försäkra sig om att meddelandena från pålitliga källor går igenom, ifall meddelandena annars skulle filtreras t.ex. till följd av felaktig spärrlistning.

Vid användning av en frilista bör man uppmärksamma att skadlig e-posttrafik också kan förmedlas via pålitliga aktörer, och man kan således inte heller förbehållslöst lita på källorna på frilistan. Dessutom kan t.ex. frilistade adresser förfalskas i skadliga e-post-

meddelanden för att göra det lättare för skadlig e-posttrafik att gå igenom. För att undvika problem bör man också följa innehållet i de meddelanden som frilistans källor sänder.

En frilista är ofta en mycket statisk lista över webbadresser. Det är tjänsteleverantörens uppgift att se till att informationen på listan är uppdaterad, så att de problem som föråldrade uppgifter medför kan undvikas.

2.3 Grålistning

Grålistning (track list, även känt som greylist) baserar sig på funktionen hos program som sänder skadlig e-posttrafik. I motsats till ett vanligt e-postsystem, försöker dessa program inte sända meddelandet på nytt, även om leveransen av meddelandet skulle misslyckas. Vid grålistning statistikförs vissa parametrar automatiskt (IP-adressen till avsändaren av inkommande e-post, adressens C-klass, SMTP-avsändare och -mottagare) eller en hashtavla som dessa ingår i. Ett meddelande från en okänd avsändare/med vissa parametrar tas inte emot. När källan efter en viss fördröjning sänder meddelandet på nytt tas det emot. I fortsättningen tas meddelanden från den ifrågavarande källan emot utan fördröjning.

Problemet med grålistning är att sakliga e-postmeddelanden från på förhand okända källor blir fördröjda. Dessutom baserar sig funktionen hos grålistning på principen att de som sänder skadliga e-postmeddelanden sänder dem endast en gång. Om de som sänder skadlig e-post försöker kringgå grålistningen genom att sända meddelandena på nytt fungerar grålistningen inte längre. Dessutom ökar återsändningen av e-postmeddelanden e-posttrafiken och belastar både nät och e-postservrar.

2.4 Omdömessystem

Omdömessystem baserar sig på meddelandekällans tidigare sändningshistorik. De meddelanden som e-postkällorna (t.ex. avsändarens IP-adress och SMTP-avsändaren) sänder följs, statistikförs och jämförs med källans tidigare meddelandehistorik. Vid statistikföring och jämförelse ägnar man uppmärksamhet åt huruvida källan sänder sakliga e-postmeddelanden eller skadliga e-postmeddelanden. E-postkällorna kan också övervakas på basis av mängden utgående meddelanden från servern. Uppgifterna används för att genom poängsättning bedöma e-postkällans omdömesnivå utifrån avsändarens tidigare sändnings- och meddelandehistorik. Omdömesnivån avgör om meddelandet från källan levereras till mottagaren på vanligt sätt, om meddelandet levereras till mottagaren med lägre prioritet eller om leveransen till mottagaren blockeras.

Fördelen med omdömessystemen är att de utnyttjar övervakning av källorna under en längre tid och att meddelandena inte filtreras på grund av enstaka osakliga meddelanden. Omdömessystemen stöder andra filtreringssystem väl och minskar som en del av heuristisk filtrering mängden fel som begås av andra kriterieuppsättningar. När omdömessystem används bör man dock beakta att systemets bedömning inte nödvändigtvis hinner reagera på den stora mängden skadlig trafik.

De omdömessystem som upprätthålls av tredje parter samlar den information de behöver för bedömningen från sina egna kunder. Uppgifterna från flera källor samlas i en gemensam databas för bedömning av omdömesnivån.

2.5 Heuristisk analys

En e-posttjänsteleverantör kan också fastställa skadligheten hos meddelanden och filtrera dem genom en analys på basis av innehållet i e-postmeddelandena eller använda

dessa metoder vid sidan om de metoder som används för att identifiera e-postkällor vid filtrering av e-postmeddelanden.

Innehållet i skadliga e-postmeddelanden uppfyller i allmänhet vissa kriterier som man känner till sedan tidigare. Filtrering som baserar sig på innehållet i ett meddelande kan ske t.ex. genom att man jämför den kontrollsumma som räknats fram ur meddelandet med kända kontrollsummor som räknats fram ur skadliga meddelanden, eller genom att man letar efter skadliga element i meddelandet, såsom vissa ord, formuleringar, bilagor, bilder eller länkar. Man kan också i ett e-postmeddelande leta efter element som tyder på att det är ett sakliga e-postmeddelande. Filtreringsmetoder som baserar sig på spärrlistor kan också kombineras med exempelvis innehållsmässig filtrering.

När flera mekanismer kombineras höjer eller sänker varje metod den skadliga nivån i meddelandet. Baserat på den slutgiltiga bedömningen av meddelandet avgörs huruvida meddelandet är skadligt eller inte. På basis av analysen spärrar filtreringsprogrammet meddelandet, märker ut det som troligen skadligt eller förmedlar meddelandet som sådant.

2.6 Avvikande trafikmängd

För att kunna identifiera avvikande trafikmängder bör en e-posttjänsteleverantör sätta gränsvärden för normal användning. Om mängden utgående e-posttrafik överskrider den gräns för sändning som definierats som normal, kan e-posttjänsteleverantören tillfälligt spärra kundens e-posttrafik. Dessutom ska e-posttjänsteleverantören om möjligt kontakta kunden, så att kunden kan vidta nödvändiga åtgärder för att avhjälpa situationen t.ex. genom att rensa den infekterade datorn.

2.7 Andra metoder som förbättrar e-posttrafikens säkerhet och tillförlitlighet

Förutom de mekanismer som nämns i föregående kapitel har en e-posttjänsteleverantör möjlighet att välja flera andra metoder för att förbättra säkerheten och tillförlitligheten hos e-posttjänsterna.

Metoder för att kontrollera om en avsändare av ett e-postmeddelanden är äkta är bl.a. Sender Policy Framework (SPF)[111] och Domain Keys Identified Mail (DKIM)[112], med hjälp av vilka man kan identifiera att ett e-postmeddelande har sänts från en e-postserver för det domännamn som e-postadressen indikerar. Som tillägg till dessa rekommenderas DMARC-protokollet, som kan användas för att följa och bestämma hur meddelanden som sänts från ett domännamn behandlas och vilka verifieringsmetoder som meddelandet borde passera. I DMARC finns även en rapporteringsegenskap, som kan användas för att följa upp hur utskick har gått igenom och förkastats.

SPF tas i bruk med hjälp av ett domännamnssystem (DNS). I domännamnssystemet publiceras en namnpost av texttyp, där man i parametrar definierar de auktoriserade e-postservrar som är tillåtna att skicka e-post i det aktuella domännamnets eller ett lägre domännamns namn. En proxyserver för e-post (MTA) bekräftar det mottagna meddelandets ursprung genom att jämföra information om returriktningen (return path) i meddelandets adressinformation med de uppgifter som publicerats i DNS-tjänsten och tillämpar de hanteringsrutiner som definierats för meddelandet, vilket leder till att det antingen godkänns, förkastas eller sätts i karantän. En svaghet med SPF är att metoden endast kontrollerar fältet return path och inte till exempel fältet för avsändare (from),

[111] IETF RFC 7208, Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1, https://tools.ietf.org/html/rfc7208.
[112] IETF RFC 6376, DomainKeys Identified Mail (DKIM) Signatures, https://tools.ietf.org/html/rfc6376.

och därför kan en skadlig avsändare ändå manipulera meddelandets kuvert och på så vis försöka vilseleda meddelandets mottagare. Detta är möjligt, eftersom slutanvändaren vanligtvis kontrollerar endast avsändarfältet då de mer detaljerade rubrikfälten som standard är dolda. Denna svaghet kan åtgärdas genom att utöver SPF även använda det andra autentiseringsprotokollet för e-post, DMARC.

DKIM är en metod för att kryptografiskt bekräfta den digitala identiteten för e-postmeddelanden, vilken typiskt är avsändarens domän. Dessutom försöker man med hjälp av metoden säkerställa att meddelandets innehåll inte har manipulerats efter att det sändes. DKIM-metoden baserar sig på en kombination av en digital underskrift och ett nyckelpar. I rubriken på meddelanden läggs en digital underskrift till som krypteras med en privat nyckel, och dessutom läggs en offentlig nyckel till i DNS-uppgifterna för det sändande domännamnet. Med den offentliga nyckeln är det möjligt för mottagarna av meddelandena att öppna uppgifterna. En DKIM-underskrift ökar eller minskar inte på egen hand meddelandets obestridlighet i någon större utsträckning, men en underskrift på ett meddelande är dock viktig information till omdömessystemen för e-post och i synnerhet för beslutsfattande som rör meddelandet. Därför ska också DKIM användas tillsammans med andra metoder som förbättrar e-postens tillförlitlighet.

Liksom SPF och DKIM baserar sig även användningen av DMARC på DNS, dvs. DMARC-poster skapas på samma sätt som andra autentiseringsprotokoll i ett domännamnssystem. Med DMARC kan man definiera det som obligatoriskt att meddelandet måste gå igenom SPF- och DKIM-valideringar. Med hjälp av DMARC är det möjligt att säkerställa att det domännamn som visas i From-fältet som användaren ser motsvarar det domännamn som har använts i SPF- och DKIM-autentiseringarna.

På samma sätt som andra kontrollmetoder för skadlig e-posttrafik har också de här mekanismerna en hel del svagheter, som bör beaktas då metoderna införs. I fråga om DKIM-metoden beskrivs detta bland annat i RFC 4686[113]. Eftersom t.ex. tjänster för förmedling av e-post, elektroniska postkort och internetaccesstjänsteleverantörers sändningstjänster förstör dessa mekanismers funktion, lämpar sig mekanismerna bäst för enbart positiv identifiering av källan.

Innan nya metoder införs ska e-posttjänsteleverantörer noggrant sätta sig in i verksamhetsprinciperna för och riskerna med metoden för att undvika felaktig filtrering av sakliga e-postmeddelanden. Ofta är det osäkert hur exakt funktionen hos enskilda metoder är om man utan förbehåll litar på den tolkning av trafikens skadlighet som metoden ger. Om flera metoder däremot används samtidigt som en del av bedömningssystemet kan mycket exakta filtreringsresultat med liten felmarginal erhållas.

3. Förhindrande av trafik med skadliga program i de domännamn eller IP-adresser som används för uppdatering av programmen

Det dåvarande Kommunikationsverket fick år 2009 kännedom om flera hundra misstänkta Conficker/Downadup-maskangrepp i de finländska näten. Antalet smittade datorer runtom i världen beräknades vara flera miljoner. Vid undersökning av nätmaskens funktion klargjordes sättet på vilket masken uppdaterades. Efter infektionen skapade masken utgående från datumet slumpmässiga domännamn som den försökte kontakta för att uppdatera sig själv. Vissa smittade terminalutrustningar kunde spåras genom att

[113] IETF RFC 4686, Analysis of Threats Motivating DomainKeys Identified Mail (DKIM), https://tools.ietf.org/html/rfc4686.

registrera några av de domännamn som masken använde och observera nättrafiken till dem. Adressuppgifterna för de smittade datorerna tillställdes dem som förvaltade näten.

Kommunikationsverket ansåg i sin tolkning (dnr 46/64/2009) att teleföretagen avsevärt kan minska det informationssäkerhetshot som maskar utgör genom att förhindra trafiken till de domännamn som används för uppdateringen av masken. När trafiken förhindras blir det avsevärt svårare att uppdatera masken och utnyttja det angripna systemet. Enligt Kommunikationsverkets tolkning kunde förhindrande av trafik mot de domännamn som används för uppdatering av det skadliga programmet anses vara en sådan nödvändig åtgärd som (enligt 272 § i den nuvarande lagen om tjänster inom elektronisk kommunikation) får vidtas för att nät- eller kommunikationstjänsten ska kunna tryggas.

Om teleföretaget vill identifiera alla smittade terminalutrustningar i sitt nät kan trafik förhindras till exempel med ett modifierat svar på en DNS-förfrågning som den smittade datorn skickat till teleföretagets resolver-namnservrar. IP-adressen för det modifierade svaret kan vara en ledig IP-adress inom teleföretagets egen IP-adressrymd.

Enligt Kommunikationsverkets tolkning hade teleföretagen rätt att lagra källadresser för trafik till de domännamn som användes för uppdatering av det skadliga programmet samt att utreda den abonnent som använder källadressen. För att utreda abonnenten fick teleföretaget också behandla förmedlingsuppgifter som det samlat i andra sammanhang. De insamlade förmedlingsuppgifterna måste förstöras genast när det inte längre fanns en grund för att behandla dem. Förmedlingsuppgifter fick ges ut till tredje parter endast på basis av de grunder som anges i lag.

År 2021 rekommenderade i sin tur Cybersäkerhetscentret vid Transport- och kommunikationsverket teleföretagen att filtrera IP-adresserna för de aktiva kommandoservrarna för det skadliga programmet Flubot, som spreds till mobiltelefoner.[114] I detta fall använde det skadliga programmet krypterad DNS-trafik, vilket innebar att blockering av trafik till använda domännamn i det fallet inte var en effektiv metod för filtrering.

4. Filtrering av SMS-trafik för att förhindra spridning av skadliga program

Cybersäkerhetscentret vid Transport- och kommunikationsverket rekommenderade år 2021 teleföretag i mobilnätet att filtrera SMS-meddelanden på basis av innehållet för att förhindra spridning av det skadliga programmet Flubot.[115] Man försökte sprida det skadliga programmet genom att skicka SMS som innehöll länkar till programmet, som man försökte få användaren att installera i sin telefon.[116] Behandling av innehållet i SMS i anknytning till sådan filtrering var möjlig inom ramarna för 272 § i lagen om tjänster inom elektronisk kommunikation.

5. Filtrering av trafik för att förhindra förberedelse till betalningsmedelsbedrägerier

År 2009 fick det dåvarande Kommunikationsverket vetskap om fall där finländska kunders nättrafik via nätbanker hade styrts till en tredje parts www-server utan att använ-

[114] FICORA #1157426 Rekommendation om filtrering av trafik inom internetaccesstjänster, 8.6.2021.
[115] FICORA #1176113 Rekommendation om filtrering av sms-trafik, 25.11.2021.
[116] Traficom, Vi publicerade en allvarlig varning om skadlig programvara som sprids via SMS, https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/vi-publicerade-en-allvarlig-varning-om-skadlig-programvara-som-sprids-sms.

daren visste om det. Styrningen hade genomförts genom att byta ut DNS-inställningarna med hjälp av ett skadligt program som installerats i användarens terminalutrustning. Därefter använde terminalutrustningen de DNS-servrar som den ansvariga för det skadliga programmet hade definierat för att utreda IP-adresser för domännamn. Förfalskningen hade antagligen gjorts med hjälp av ett skadligt program av typen DNS Changer (t.ex. Zlob).

Enligt Kommunikationsverkets tolkning (dnr 1952/64/2009) kunde teleföretagen med stöd av 272 § i den nuvarande lagen om tjänster inom elektronisk kommunikation filtrera trafik till domäner som specificeras från fall till fall, för att förhindra förberedelse till betalningsmedelsbedrägerier enligt 37 kap. 11 § i strafflagen, vilka planeras bli genomförda i omfattande utsträckning via kommunikationstjänsterna. Filtrering är motiverad även för att upptäcka, förhindra och utreda störningar som kan inverka menligt på informationssäkerheten och för att möjliggöra undersökning av störningarna.

Enligt lagen om tjänster inom elektronisk kommunikation får förmedlingsuppgifter behandlas i den utsträckning som det behövs för att producera och använda nättjänster, kommunikationstjänster eller mervärdestjänster samt för att sörja för informationssäkerheten på det sätt som anges i lag. Infekterade terminalutrustningar i teleföretagets nät äventyrar informationssäkerheten hos teleföretagets tjänster. Därför kan det antas att en utredning av de terminalutrustningar som blivit infekterade av skadliga program är en nödvändig åtgärd i syfte att utföra tjänsten och att sörja för tjänstens informationssäkerhet.

Enligt Kommunikationsverkets tolkning kunde teleföretag samla in de källadresser för trafik till specificerade nätområden som har samband med fallet och klarlägga den abonnent som använder källadressen på basis av uppgifter som lagrats i en DHCP-logg (eller en motsvarande logg).

6. Rekommendationer för informationssäkerheten i Ethernet-gränssnitt

Detta kapitel behandlar några av de viktigaste informationssäkerhetsproblemen i Ethernet-teknik som påverkar kommunikationsnätens och -tjänsternas funktion samt exempel på hur dessa problem kan avvärjas. Exemplen gäller situationer där teleföretagets nät har genomförts med traditionella switchar. De problem som beskrivs gäller således i allmänhet inte nät som använder t.ex. MPLS- eller pseudowire-tunnling.

Transport- och kommunikationsverket rekommenderar att teleföretagen förbereder sig också för de hot som nämns i detta kapitel när de genomför behövliga skyddsmekanismer, trots att föreskriften inte ger några detaljerade skyldigheter i frågan.

6.1 Sändningsstormar

En sändningsstorm uppstår när en för stor mängd multicastmeddelanden sänds till nätet via en port i samtrafikgränssnittet. Sändningsstormen kan göra samtrafikgränssnittet oanvändbart om multicastmeddelandena fyller det sammankopplade nätets kapacitet. Därför ska parter som bedriver samtrafik förbereda sig på att begränsa konsekvenserna av sändningsstormar. Begränsningen kan genomföras exempelvis genom att begränsa den kapacitet som spridningsmeddelandena får i nätverket.

Transport- och kommunikationsverket rekommenderar att man i samtrafikgränssnitt skulle använda endast sådana switchar som stöder så kallad stormkontrollfiltrering. Med hjälp av denna filtrering är det möjligt att begränsa en viss andel av linjekapaciteten för

unicast- och broadcastsändningar. Filterinställningarna måste göras så att filtrering inte medför olägenhet på normal trafik i nätet.

6.2 L2-styrprotokoll

Med ett Spanning Tree-protokoll (STP) kan en operatör förebygga slingor i sitt L2-nät. Protokollet kan också medföra avsevärda problem om det används fel. Även många tillverkarspecifika protokoll, t.ex. Ciscos CDP eller VTP, kan orsaka motsvarande problem. I värsta fall kan kunden avsiktligen eller oavsiktligen krascha tjänsten eller obehörigt styra trafik via sitt eget abonnemang, vilket möjliggör t.ex. avlyssning och modifiering av trafiken. STP- och tillverkarspecifika protokoll ska därför isoleras på styrnivå.

6.3 VLAN hopping

Med paket som är försedda med två VLAN-taggar (Double Tag VLAN) är det möjligt att sända blockeringsattacker från en kundport mot en switch i stamnätet och ända till VLAN som finns bakom andra switchar. Det är möjligt, eftersom switchen i en normal Ethernet-anslutning tar bort endast den yttre VLAN-taggen, vilket betyder att ännu en andra VLAN-tagg kvarstår i paketet. Det går inte att bilda en dubbelriktad förbindelse, men på detta sätt är det möjligt att göra ett överbelastningsangrepp mot en port för en annan tjänst eller kund.

I syfte att förebygga hotet ska nätoperatören säkerställa att endast de VLAN som en abonnent har i användning är tillåtna i en abonnentswitchs stamport. I samtrafikgränssnittet ska nätoperatören tillåta endast det intervall för VLAN-id som överenskommits med tjänsteoperatören. Det rekommenderas också att antalet switchar mellan routerutrustning och kundutrustning hålls så litet som möjligt.

6.4 Drifthantering och filtrering av MAC-adresser

Drifthantering och filtrering av MAC-adresser är metoder för skyddande av nät som behövs när man skyddar sig mot störande teletrafik och fel som trasig utrustning orsakar. Om en MAC-tabell för en switch blir fylld av adresser, distribuerar switchen alla paket till varje switchport. Det betyder att varje enhet som kopplats till switchen ser all kundtrafik som passerar via switchen. MAC-tabellens begränsade storlek i switchar och DSLAM är alltså ett av de kända informationssäkerhetshoten.

Problemets storlek beror dock på den teknik som använts. Teleföretaget kan minska problemen till exempel genom att utnyttja Provider Backbone Bridging-teknik (802.1ah).[117] Problemet kan också förhindras genom att begränsa antalet portspecifika MAC-adresser och genom att tillåta trafik endast till korrekta och inlärda MAC-adresser. I äldre eller förmånligare switchar är det inte alltid möjligt att förhindra att MAC-tabellerna fylls av kundportar.

Detta problem gäller också dimensioneringen av Ethernet-nätet mellan termineringsroutern och kundterminalen. Nät- och tjänsteoperatören bör kunna hantera antalet aktiva MAC-adresser för varje specifik port (abonnentswitch eller samtrafikgränssnitt).

[117] IEEE Standards Association, IEEE Std. 802.1ah – Provider Backbone Bridges, https://www.ieee802.org/1/.

7. Rekommendationer om information om informationssäkerhet

7.1 Allmän information om informationssäkerhetsrisker och de skyddsmetoder som finns tillgängliga för kunden

Om kunden skyddar sin terminalutrustning dåligt och använder tjänster ovarsamt äventyras informationssäkerheten inte bara i kundens egen terminalutrustning, utan även i tjänster som teleföretaget tillhandahåller samt för andra användare.

Det rekommenderas att teleföretag producerar förhandsinformation till kunderna om hur kommunikationstjänsten eller abonnemanget ska användas så att informationssäkerheten säkerställs. Med allmän information om informationssäkerhet till kunder ökar teleföretaget kundernas medvetenhet om de allmänna risker som hänför sig till nätens och tjänsternas informationssäkerhet. Det är möjligt att undvika en betydande del av de rapporterade problemen, om kunderna på ett behörigt sätt ser till att terminalutrustningen har ett grundläggande skydd och att tjänster används med beaktande av hot mot informationssäkerheten.

Målet med informationen är också att kunderna ges möjlighet att skydda sig mot informationssäkerhetshot som berör en specifik abonnemangstyp. Teleföretaget bör därför se till att kunden blir informerad om dessa hot samt om de informationssäkerhetsåtgärder som kunden kan vidta innan abonnemanget kopplas.

Teleföretaget kan informera på olika sätt. Det är möjligt att ordna informationen exempelvis med hjälp av en inloggningssida som möjliggör kontakt eller genom att hänvisa kunden till en viss webbplats. Teleföretaget kan förutom genom sin egen kundinformation till, även hänvisa kunden till webbplatsen för Cybersäkerhetscentret vid Transport- och kommunikationsverket.

Informationen ska fokusera på de åtgärder som kunden eller användaren av ett kundabonnemang kan vidta för att sörja för informationssäkerheten i sin egen terminalutrustning. Sådana åtgärder är att till exempel kryptera trafiken, skilja åt användarnas trafik, ta i bruk en brandvägg innan datorn ansluts till nätet, skaffa virusskydd samt uppdatera operativsystemet och andra program.

Vid behov ska informationen fokusera på informationssäkerhetsrisker som är specifika för varje abonnemangstyp och som avser särskilda risker som hänför sig till det tekniska sättet att tillhandahålla abonnemanget. Ett exempel på en risk är att tillhandahålla internetaccesstjänster med hjälp av en okrypterad WLAN-förbindelse. I sådana situationer ska teleföretaget informera om de särskilda risker för kommunikationens konfidentialitet som hänför sig till användningen av abonnemanget. Även abonnemang där användarna delar på kapaciteten kan vara förknippade med informationssäkerhetsrisker.

Bestämmelser om information till kunden finns även i 246.3 § i lagen om tjänster inom elektronisk kommunikation. Enlig den ska abonnenterna administrera utrustning och system som ansluts till ett allmänt kommunikationsnät i enlighet med teleföretagets anvisningar så att de inte äventyrar informationssäkerheten i allmänna kommunikationsnät och -tjänster. Därtill föreskrivs i 274 § 2 mom. i lagen om tjänster inom elektronisk kommunikation om teleföretagets skyldighet att informera om vilka skyddsåtgärder som kan vidtas, när teleföretaget informerar abonnenten eller användaren om en informationssäkerhetsincident eller hotet om en sådan som riktar sig mot teleföretagets tjänst.

7.2 Allmän information om informationssäkerhetsåtgärder

Det rekommenderas att teleföretag producerar förhandsinformation till kunderna om hurdana åtgärder som kan vidtas till följd av eventuell användning av det allmänna kommunikationsnätet eller -tjänsten som äventyrar informationssäkerheten.

I statsrådets förordning om information som ska ges innan avtal om kommunikationstjänster ingås (96/2021) föreskrivs också att teleföretaget innan ett avtal om kommunikationstjänster ingås ska ge konsumenten information om tjänsteleverantörens åtgärder om informationssäkerheten är hotad eller när hot eller sårbarheter som gäller informationssäkerheten uppstår (1 § 6 punkten). Teleföretaget ska för kunderna även göra upp en beskrivning av de allmänna principer som tillämpas när det blir nödvändigt att ingripa i användning av abonnemanget eller tjänsterna som äventyrar kommunikationstjänsternas informationssäkerhet. Detta innebär att kunderna ska informeras om t.ex. att kundens abonnemang kan stängas av tillfälligt om en infekterad terminal kopplas till abonnemanget.

7.3 Information om sårbar kundutrustning

Användare av kommunikationstjänster kan spela en stor roll i skyddet mot informationssäkerhetshot som hänför sig till kommunikationsnäten och -tjänsterna.[118]

I 274 § i lagen om tjänster inom elektronisk kommunikation föreskrivs om teleföretags störningsanmälningar till abonnenter och användare i situationer där teleföretagets tjänster är utsatta för betydande kränkningar av eller hot mot informationssäkerheten eller för någonting annat som gör att kommunikationstjänsterna inte fungerar eller väsentligen stör dem. I 246 § 3 mom. i lagen i sin tur föreskrivs att abonnenterna ska administrera utrustning och system som ansluts till ett allmänt kommunikationsnät i enlighet med teleföretagets anvisningar så att de inte äventyrar informationssäkerheten i det allmänna kommunikationsnätet och i de allmänna kommunikationstjänsterna.

Sårbar kundutrustning utgör ett hot både för kundens informationssäkerhet och för informationssäkerheten i teleföretagets kommunikationsnät och -tjänster. I synnerhet i takt med att mängden utrustning i 5G-näten mångdubblas är det bra att även med hjälp av kontroller i näten förbereda sig för signalstormar i situationer där en stor mängd sårbar kundutrustning infekteras av ett skadligt program. Därtill är det bra att ägna uppmärksamhet åt uppdatering eller avlägsnande av sårbar utrustning från kommunikationsnätet.

Transport- och kommunikationsverket rekommenderar att teleföretaget informerar sin kund när teleföretaget blir medvetet om att kunden har sårbar terminalutrustning, vars sårbarhet hotar kundens informationssäkerhet eller informationssäkerheten i teleföretagets kommunikationsnät eller -tjänst, även i de fall där det enligt lag inte finns någon skyldighet att göra detta. I sårbarheter som äventyrar informationssäkerheten kan man från fall till fall ingripa även med hjälp av åtgärder i enlighet med 272 och 273 § i lagen om tjänster inom elektronisk kommunikation samt punkterna 22 och 23 i föreskriften.

[118] ENISA GL SO29 gäller information till användarna om informationssäkerhetshot och vilka åtgärder som finns tillgängliga för användarna för att de ska kunna skydda sig mot dem.

7.4 Beskrivning av principerna för filtrering av e-posttjänster

Kunden har rätt att få information om vilka filtreringsprinciper som det teleföretag som tillhandahåller e-posttjänsten tillämpar.[119]

Filtreringen av e-posttrafik föranleder ofta frågor från kunderna till tjänsteleverantören om sakliga e-postmeddelanden filtreras felaktigt eller om exempelvis mängden skadlig inkommande e-posttrafik till kundens e-postlåda ökar markant. Eftersom identifiering och filtrering eller utmärkning av skadlig eposttrafik är nödvändig för att säkerställa e-posttjänstens funktion och tillgänglighet, kan missförstånd och onödiga kundreklamationer undvikas genom att kunderna informeras om grundprinciperna för filtreringen av e-posttrafik.

Det rekommenderas att teleföretaget för sina kunder beskriver vilka allmänna principer för filtrering av e-post som företaget tillämpar. Syftet med beskrivningen är att man rent allmänt berättar för kunden om de filtreringsmetoder som används och hur metoderna inverkar på kundens trafik. Beskrivningen av filtreringsprinciperna för kunden får dock inte äventyra kommunikationstjänstens informationssäkerhet. Beskrivningen behöver inte vara onödigt detaljerad med exakta uppgifter om t.ex. de grunder på vilka ett enskilt e-postmeddelande på basis av innehållet bedöms som skadlig trafik. Om t.ex. spärrlistor används behöver e-posttjänsteleverantören inte i detalj räkna upp de spärrlistor som används vid filtrering, eftersom de listor som används kan variera från fall till fall.

7.5 Beskrivning av administreringen av e-postadresser

Praxis för administrering av e-postadresser varierar från en tjänsteleverantör till en annan. Det är möjligt att undvika missförstånd och påskynda problemlösningen genom att definiera praxis för administrering och beskriva den för kunderna.

Det rekommenderas att ett teleföretag som tillhandahåller e-posttjänster för kunderna ska beskriva vilka praxis det tillämpar för administrering av e-postadresser. Med hjälp av beskrivningen ska kunden få veta hur han eller hon kan få en ny e-postadress, ändra e-posttjänstens inställningar och ta en e-postadress ur bruk.

[119] Bestämmelser om vilken information som ska ges om behandlingen av förmedlingsuppgifter finns i 138.2 § i lagen om tjänster inom elektronisk kommunikation. Se även 1 § 6 punkten i ovannämnda statsrådets förordning om information som ska ges innan avtal om kommunikationstjänster ingås (96/2021).