

**MOTIVERING TILL OCH TILLÄMPNING AV
FÖRESKRIFT 13**

**OM INTERNETFÖRBINDELSE-
TJÄNSTERNAS INFORMATIONSSÄKERHET**

INNEHÅLL

INNEHÅLL	2
1 LAGSTIFTNING	3
1.1 RÄTTSGRUND	3
1.2 ANDRA RELATERADE BESTÄMMELSER	4
1.3 KOMMUNIKATIONSVÄRKETS TOLKNINGAR	5
2 SYFTET MED FÖRESKRIFTEN OCH ÄNDRINGSHISTORIA	7
2.1 SYFTET MED FÖRESKRIFTEN	7
2.2 CENTRALA ÄNDRINGAR OCH ÄNDRINGSHISTORIA	7
3 1 § TILLÄMPNINGSOMRÅDE	8
4 2 § DEFINITIONER	8
4.1 INTERNETFÖRBINDELSETJÄNST	8
4.2 KUNDANSLUTNING.....	8
4.3 TJÄNSTER I EN KUNDANSLUTNING.....	9
4.4 SKADLIG TRAFIK	9
4.5 FILTRERING	9
5 3 § KUNDANSLUTNINGARNAS INFORMATIONSSÄKERHET	9
5.1 ATT SKILJA ANVÄNDARNAS TRAFIK FRÅN VARANDRA	9
6 4 § INFORMATION	10
6.1 INFORMATION TILL KUNDEN.....	10
6.2 KUNDINFORMATION OM ANSLUTNINGENS TEKNISKA BEGRÄNSNINGAR	11
7 5 § DIRIGERING OCH ROUTNING AV E-POSTTRAFIK FRÅN KONSUMENTANSLUTNING	12
7.1 FÖRHINDRANDE AV OBEGRÄNSAD SMTP-TRAFIK FRÅN KONSUMENTANSLUTNING	12
7.2 TILLÅTEN SMTP-TRAFIK FRÅN KONSUMENTANSLUTNING I SPECIELLA FALL.....	12
8 6 § UPPTÄCKT AV SKADLIG TRAFIK	13
8.1 UPPTÄCKT AV SKADLIG TRAFIK.....	13
9 7 § FILTRERING AV SKADLIG TRAFIK	13
9.1 PROCESSER OCH HANDLINGSMÖNSTER FÖR TILLFÄLLIG FILTRERING AV TRAFIKEN.....	14
9.2 FILTRERING AV TRAFIK SOM INNEHÅLLER FELAKTIGA KÄLLADRESSER.....	14
9.3 IDENTIFIERING AV EN ANVÄNDARE	15
9.4 ADRESS- OCH RUTTFILTRERING.....	15
9.5 GENOMFÖRANDE AV FILTRERINGSÅTGÄRDER	16
10 8 § FRÅNKOPPLING AV ANSLUTNINGEN	16
10.1 FRÅNKOPPLING AV KUNDANSLUTNINGAR	16
10.2 ANVISNINGAR FÖR FRÅNKOPPLINGSPROCESSEN.....	16
11 9 § BEHANDLING OCH STATISTIKFÖRING AV KRÄNKNINGAR AV INFORMATIONSSÄKERHET ...	17
11.1 KONTAKTADRESSER FÖR ANMÄLNING AV KRÄNKNINGAR AV INFORMATIONSSÄKERHET	17
11.2 BEHANDLING AV KRÄNKNINGAR AV INFORMATIONSSÄKERHET	18
11.3 STATISTIKFÖRING AV ANMÄLNINGAR	19
12 10 § IKRAFTTRÄDANDE OCH ÖVERGÅNGSBESTÄMMELSER	20
13 REFERENSLISTA	20

1 LAGSTIFTNING

Syftet med detta kapitel är att ge föreskriftens användare en helhetsbild av de författningar som utgör grunden för föreskriften. Här uppräknas också andra väsentliga författningar som har samband med ämnet.

1.1 Rättsgrund

Kommunikationsverkets föreskrift baserar sig på lagen om dataskydd vid elektronisk kommunikation (516/2004 jämte ändringar [1]), som trädde i kraft den 1 september 2004 och verkställde för sin del EG:s direktiv om integritet och elektronisk kommunikation som godkändes i juli 2002.

Kommunikationsverkets föreskrift baserar sig också på kommunikationsmarknadslagen (393/2003 jämte ändringar [3]), som trädde i kraft den 25 juli 2003 och verkställde för sin del EG:s direktiv inom elektronisk kommunikation, dvs. ramdirektiv, auktorisationsdirektiv, tillträdesdirektiv och direktiv om samhällsomfattande tjänster vilka godkändes i februari 2002.

Med stöd av 19 § 1 mom. i lagen om dataskydd vid elektronisk kommunikation ska ett teleföretag handha dataskyddet för sina tjänster. Handhavandet av dataskyddet för tjänster och behandling avser åtgärder för att trygga säkerheten av verksamheten, datatrafiken, utrustningen och programmen samt för datamaterialet. Åtgärder som vidtas för att handha dataskyddet ska anpassas till de hot som föreligger samt till den tekniska utvecklingens nivå och till kostnaderna. 19 § i lagen om dataskydd vid elektronisk kommunikation: Med stöd av 3 mom. är ett teleföretag gentemot abonnenterna och användarna ansvarigt för det dataskydd som avses i 1 mom. också i fråga om sådan tredje part som helt eller delvis utför nättjänsten, kommunikationstjänsten, lagringen av uppgifter eller mervärdestjänsten.

Kommunikationsverket kan med stöd av 19 § 4 mom. i lagen om dataskydd vid elektronisk kommunikation ge teleföretag närmare föreskrifter om ovan i 1 och 3 mom. avsett dataskydd för tjänster.

Med stöd av lagens 20 § 1 mom. har ett teleföretag samt den som handlar för dess räkning rätt att vidta nödvändiga åtgärder enligt 2 mom. med avseende på dataskyddet:

- 1) för att upptäcka, förhindra och utreda störningar som kan inverka menligt på dataskyddet i kommunikationsnäten eller för de tjänster som anslutits till dem och för att möjliggöra undersökning av störningarna,
- 2) för att trygga kommunikationsmöjligheterna för den som sänder eller tar emot ett meddelande, eller
- 3) för att förhindra förberedelse till betalningsmedelsbedrägerier enligt 37 kap. 11 § i strafflagen, vilka planeras bli genomförda i omfattande utsträckning via kommunikationstjänsterna.

Enligt lagens 20 § 2 mom. kan de åtgärder som avses i 1 mom. omfatta:

- 1) en 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 dataskyddet,
- 4) andra jämförbara åtgärder av teknisk natur.

Enligt 20 § 3 mom. i lagen om dataskydd vid elektronisk kommunikation, om det på basis av 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 paragrafens 1 mom. inte kan säkerställas genom en automatisk analys av innehållet, får innehållet i det enskilda meddelandet behandlas manuellt. Avsändaren och mottagaren av meddelandet ska underrättas om den manuella behandlingen av innehållet, förutom om det är sannolikt att underrättelsen äventyrar uppnåendet av målen enligt 1 mom.

Enligt lagens 20 § 4 mom. ska åtgärderna enligt denna paragraf utföras omsorgsfullt och de ska stå i rätt proportion till den störning som avvärjs. Åtgärderna får inte begränsa yttrandefriheten, skyddet av konfidentiella meddelanden eller integritetsskyddet mer än nödvändigt med tanke på

säkerställandet av möjligheterna att uppnå målen enligt 1 mom. Åtgärderna ska avbrytas, om det inte längre finns i denna paragraf nämnda förutsättningar för att vidta dem.

Enligt 20 § 5 mom. kan Kommunikationsverket meddela teleföretagen närmare föreskrifter om hur åtgärderna enligt denna paragraf ska genomföras tekniskt.

Enligt 128 § i kommunikationsmarknadslagen ska allmänna kommunikationsnät och kommunikationstjänster samt kommunikationsnät och kommunikationstjänster som ansluts till dem planeras, byggas och underhållas bland annat så att

4) användarnas eller andra personers datasekretess, dataskydd eller andra rättigheter inte äventyras.

I lagens 129 § sägs att Kommunikationsverket kan meddela föreskrifter enligt 128 § om kvalitetskrav på kommunikationsnät och kommunikationstjänster samt om kompatibilitet. Föreskrifterna kan gälla

10) säkerhet och störningsfrihet i kommunikationsnät,

16) underhåll och uppföljning av prestanda samt nätverksadministration,

17) teknisk dokumentation.

1.2 Andra relaterade bestämmelser

1.2.1 Kommunikationsmarknadslagen

67 § Avtal om kommunikationstjänster. En ändring i paragrafen förbereds vilket medför att flera omständigheter än tidigare ska behandlas i avtal om kommunikationstjänster. Nedan finns de nya punkter som kan vara av betydelse vid tillhandahållandet av internetförbindelsetjänster:

I ett avtal ska åtminstone nämnas:

[...]

15) uppgifter om de förfaranden för att mäta och styra trafiken som teleföretaget använder för att undvika överbelastning av nätet,

16) information om hur förfarandena enligt 15 punkten kan inverka på tjänsternas kvalitet,

[...]

18) begränsningar när det gäller användningen av en levererad terminal,

[...]

21) vilka åtgärder teleföretaget kan vidta om datasäkerheten är hotad.

131 § Skyldighet att undanröja störning. I 1 mom. konstateras att om ett kommunikationsnät eller en utrustning orsakar fara eller störning för ett kommunikationsnät, utrustning, kommunikationsnätets användare eller någon annan person, ska teleföretaget eller någon annan innehavare av kommunikationsnätet eller utrustningen omedelbart vidta åtgärder för att korrigera situationen och vid behov koppla bort kommunikationsnätet eller utrustningen från det allmänna kommunikationsnätet.

Kommunikationsverket kan i det fall som avses i 131 § 1 mom. bestämma om korrigeringsåtgärder samt om bortkoppling av nätet eller utrustningen.

1.2.2 Kommunikationsverkets tekniska föreskrifter

Föreskrift 9 om skyldighet att anmäla kränkningar av informationssäkerhet i allmän televerksamhet [4]. Föreskriften tillämpas på allmän televerksamhet. Syftet med föreskriften är att definiera förfaringsätt och innehåll i de anmälningar som teleföretagen ger till Kommunikationsverket och till kunderna, om teleföretagets tjänst är utsatt för en betydande kränkning av informationssäkerheten eller föremål för ett hot mot informationssäkerheten så som avses i 21 § i lagen om dataskydd vid elektronisk kommunikation.

Föreskrift 11 om e-posttjänsternas informationssäkerhet och funktionsduglighet [5]. Föreskriften tillämpas på produktion av e-posttjänster som tillhandahålls i allmänna kommunikationsnät samt på system, kommunikationsnät och kommunikationstjänster som en leverantör av e-posttjänster använder för detta ändamål. Syftet med föreskriften är att säkerställa att konsumenterna har fungerande e-posttjänster.

Föreskrift 28 om interoperabilitet av kommunikationsnät och kommunikationstjänster [6]. Föreskriften tillämpas på allmänna kommunikationsnät och kommunikationstjänster samt på

myndighetsnät. Föreskriftens 2 kap. tillämpas på kommunikationstjänster som tillhandahålls i telefonnätet. Syftet med föreskriften är att främja sammankoppling av olika teleföretags kommunikationsnät och -tjänster samt interoperabilitet av kommunikationstjänster från ända till ända.

Följande ärenden som nämns i 4 § i föreskrift 28 har samband med föreskrift 13: skyldigheter som gäller förhindrande av trafik som innehåller felaktiga källadresser, filtrering av felaktig ruttannonsering samt dokumentation av IP-adressblock. Till samma helhet hör också de nya skyldigheter som åläggs i föreskriftens 3 § och som gäller informations säkerhet hos kund- och sammankopplingsgränssnitt samt tolerans mot och förhindrande av störningar.

Föreskrift 47 om hantering av teleföretagens informationssäkerhet [7]. Föreskriften tillämpas på teleföretagens åtgärder som hänför sig till att genomföra allmänna nät- och kommunikationstjänster. Föreskriften omfattar till exempel tillhandahållandet av internetförbindelsetjänster och e-posttjänster samt taltelefonitjänster i enlighet med kommunikationsmarknadslagen. I föreskriften åläggs teleföretagen informationssäkerhetskrav som de bör beakta när de organiserar sin verksamhet.

Föreskrift 57 om underhåll av kommunikationsnät och -tjänster samt om förfarande vid fel och störningar [8]. Föreskriften tillämpas på alla allmänna kommunikationsnät och kommunikationstjänster som näten tillhandahåller. Syftet med föreskriften är att förbättra teleföretagens beredskap inför fel och störningar och procedurer vid fel och störningar.

1.3 kommunikationsverkets tolkningar

Kommunikationsverket har gett flera tolkningar av tillämpningen av 20 § i lagen om dataskydd vid elektronisk kommunikation. Några av dem har publicerats på CERT-FI:s webbplats under avsnittet Ohjeet (på finska) <http://www.cert.fi/ohjeet.html>. Avsnittet kompletteras regelbundet med nya tolkningar.

1.3.1 Behandlingen av identifieringsuppgifter i syfte att handha dataskyddet (387/64/2009)

Vissa teleföretag har informerat Kommunikationsverket om tolkningsproblem som hänför sig till de verkningar som ändringen av lagen om dataskydd vid elektronisk kommunikation har på behandlingen av identifieringsuppgifter i syfte att handha informationssäkerhet. Tolkningsproblemen gäller situationer där teleföretaget av informationssäkerhetsskäl ska kunna identifiera en kund som har använt en viss IP-adress genom att behandla identifieringsuppgifter som lagrats i en DHCP-logg. Det är nödvändigt att kunna identifiera kunden för att informationssäkerhetsåtgärderna ska kunna riktas till rätt kundanslutning.

Enligt Kommunikationsverkets tolkning får ett teleföretag behandla identifieringsuppgifter vid behov både i situationer som definieras i 20 § 1 mom. lagen om dataskydd vid elektronisk kommunikation och när det vidtar sådana åtgärder som avses i paragrafens 2 mom. Enligt Kommunikationsverkets tolkning får teleföretaget behandla identifieringsuppgifter förutom vid utförandet av en åtgärd som avses i 20 § också vid förberedande åtgärder som är nödvändiga för att den egentliga åtgärden kan 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.

1.3.2 Förhindrande av trafik från skadliga program (46/54/2009)

CERT-FI har fått vetskap om att flera hundra datorer har blivit smittade av masken Conficker/Downadup i finländska nät. Antalet smittade datorer runtom i världen beräknas vara flera miljoner. Vid undersökning av nätmaskens funktion har man klargjort sättet med vilket masken uppdateras. Efter infektionen skapar masken utgående från datumet slumpmässiga domännamn som den försöker kontakta för att kunna uppdatera sig själv. Vissa smittade terminalutrustningar har spårats genom att registrera några av de domännamn som masken använder och genom att observera nättrafiken till dem. Adressuppgifterna till de smittade datorerna har tillställts dem som upprätthåller näten.

Enligt Kommunikationsverkets tolkning kan teleföretagen avsevärt minska det informationssäkerhets hot som masken orsakar genom att förhindra trafiken till de domännamn som används för uppdateringen av masken. Då trafiken förhindras blir det avsevärt svårare att uppdatera masken och utnyttja det angripna systemet. Enligt Kommunikationsverkets tolkning kan

förhindrande av trafik mot de domännamn som används för uppdatering av det skadliga programmet anses vara en sådan nödvändig åtgärd som enligt lag 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 resolver-namnservrarna. IP-adressen för det modifierade svaret kan vara en ledig IP-adress inom teleföretagets eget IP-adressrymd.

Enligt Kommunikationsverkets tolkning har teleföretagen rätt att lagra källadresser för trafik till de domännamn som används för uppdatering av det skadliga programmet samt att utreda den abonnent som använder källadressen. För att utreda abonnenten får teleföretaget också behandla identifieringsuppgifter som det samlat i andra sammanhang. De insamlade identifieringsuppgifterna måste förstöras genast när det inte längre finns en grund för att behandla dem. Identifieringsuppgifter får ges ut till tredje parter endast på basis av de grunder som ges i lag.

1.3.3 Smittad terminalutrustning är alltid ett informationssäkerhetshot (46/64/2009)

Kommunikationsverkets vedertagna tolkning avser att smittade 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 handa tjänstens informationssäkerhet.

1.3.4 Filtrering av trafik (1952/64/2009)

CERT-FI har fått vetskap om fall där finländska kunders nättrafik via nätbanker har styrts till en tredje parts www-server utan att användaren vet om det. Styrningen har genomförts genom att byta ut DNS-inställningarna med hjälp av ett skadligt program som installerats i användarens terminalutrustning. Därefter använder terminalutrustningen de DNS-servrar som det skadliga programmets upprätthållare har definierat för att utreda IP-adresser för domännamn. Förfalskningen har antagligen gjorts med hjälp av ett skadligt program av typen DNS Changer (t.ex. Zlob).

Enligt Kommunikationsverkets tolkning kan teleföretagen med stöd av lagen om dataskydd vid elektronisk kommunikation filtrera trafik till de nätområden som ges i den tekniska bilagan för att förhindra förberedelse till betalningsmedelsbedrägerier enligt 37 kap. 11 § i strafflagen, vilka planeras bli genomförda i omfattande utsträckning via kommunikationstjänsterna. Filtrering är motiverad också för att upptäcka, förhindra och utreda störningar som kan inverka menligt på dataskyddet och för att möjliggöra undersökning av störningarna.

Enligt lagen om dataskydd vid elektronisk kommunikation får identifieringsuppgifter behandlas i den utsträckning det är nödvändigt för att utföra och använda nättjänster, kommunikationstjänster eller mervärdestjänster och för att sörja för dataskyddet på det sätt som anges i lag. Smittade 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 handa tjänstens informationssäkerhet.

Enligt Kommunikationsverkets tolkning kan teleföretag samla in källadresser för trafik till de nätområden som ges i bilagan och klarlägga abonnenten som använder källadressen på basis av uppgifter som lagrats i en DHCP-logg (eller en motsvarande logg).

1.3.5 Identifiering av en användare som stör tjänsten för en tredje part (268/64/2010)

Vissa teleföretag har bett om Kommunikationsverkets åsikt beträffande rätten att behandla identifieringsuppgifter för att identifiera en kund som stör tjänsten för en tredje part. En störande kund använder en kommunikationstjänst som förverkligats med hjälp av en IP-adress som ofta byts ut. Användning av dynamiska adresser leder till att tjänsteleverantören som störs inte kan rikta sina begränsningsåtgärder mot störaren på basis av nätadressen. Likaså är det omöjligt för teleföretaget att identifiera någon som använder en sådan adress enbart utgående från kunduppgifterna.

Enligt Kommunikationsverkets uppskattning kan sådan användares verksamhet som avsevärt och omedelbart begränsar andra användares möjligheter att använda kommunikationstjänsten antas innebära en sådan störning som orsakar skada för kommunikationstjänsten och ger rätt till att vidta informationssäkerhetsåtgärder så som avses i lagen om dataskydd vid elektronisk kommunikation. Att vidta åtgärder med avseende på dataskyddet kan anses vara motiverat också för att trygga kommunikationsmöjligheterna för andra användare.

Vid bedömningen av begränsningen av användningsmöjligheterna ska man fästa uppmärksamhet vid att den nytta som åtgärderna ger ska vara avsevärt större än den skada som äventyrar skyddet av konfidentiella meddelanden. Vid bedömningen är det skäl att fästa uppmärksamhet åtminstone vid tjänstens betydelse samt vid sannolikheten av eventuella begränsningar och inverkan bland användarna.

När teleföretaget bedömer hur direkta begränsningarna av användningsmöjligheterna är, ska det samtidigt beakta hur sannolika begränsningsåtgärderna är. Bedömningen av hur direkta begränsningarna är baserar sig generellt på egen erfarenhet av begränsningsåtgärdernas sannolikhet hos den som bedömer behandlingsbehovet. Om teleföretaget redan har vidtagit några begränsningsåtgärder är det inte nödvändigt att bedöma hur direkta de är.

Enligt Kommunikationsverkets tolkning kan användare som stör en tredje parts tjänst identifieras genom att behandla identifieringsuppgifter då man beaktar ovan nämnda villkor. En förutsättning för behandlingen av identifieringsuppgifterna är dock alltid att målet, som behandlingen avser, inte kan nås på andra sätt. En lindrigare åtgärd än en begränsning av kommunikationsmöjligheter är identifiering av en användare som sedan kan kontaktas.

1.3.6 Definition av meddelande inom ramen för lagen om dataskydd vid elektronisk kommunikation

I lagen om dataskydd vid elektronisk kommunikation avses med *meddelande* samtal, elektronisk post, textmeddelande, talmeddelande och annat motsvarande meddelande som i ett kommunikationsnät förmedlas mellan parterna eller till en mottagarkrets som inte är utvald på förhand. Enligt Kommunikationsverkets tolkning är alla meddelanden och budskap i kommunikationsnäten sådana meddelanden som avses i lagen om dataskydd vid elektronisk kommunikation oberoende av om det är fråga om meddelanden som fysiska personer eller olika system skickar varandra.

2 SYFTET MED FÖRESKRIFTEN OCH ÄNDRINGSHISTORIA

Syftet med detta kapitel är att informera användaren om föreskriftens mål och syften. I kapitlet behandlas också de mest betydande ändringarna av tidigare skyldigheter och rekommendationer.

2.1 Syftet med föreskriften

Syftet med denna föreskrift är att främja internetförbindelsetjänsternas informationssäkerhet. Målet är att förebygga informationssäkerhetsproblem i internetförbindelsetjänster och främja ibruktage av nya informationssäkerhetstjänster. Avsikten är att säkerställa att teleföretagen handhar informationssäkerheten i samband med sina internetförbindelsetjänster, vilket förbättrar kommunikationstjänsternas driftsäkerhet och tillförlitlighet.

Syftet med föreskriften och de rekommendationer som ges i samband med den är också att främja de lösningar som enligt teleföretagen är bra. En enhetlig och grundläggande informationssäkerhetsnivå för internetförbindelsetjänster är till fördel för alla aktörer och teleföretag i branschen.

2.2 Centrala ändringar och ändringshistoria

Skyldigheter och rekommendationer som tar ställning till IP-samtrafik har tagits bort från föreskrift 13 A/2008 M och fogats till föreskrift 28 H/2010 M.

Bestämmelserna i 3 § i föreskrift 13 A/2008 M har omgrupperats. Beskrivningen på skyldigheter att informera om informationssäkerhetsrisker har flyttats till 4 §.

Bestämmelser om förhindrande av SMTP-trafik till konsumentanslutningar som fanns i 4 § i föreskrift 13 A/2008 M har tagits bort. Bestämmelsen har i praktiken förbjudit SMTP-servrar som finns bakom konsumentanslutningar. De bestämmelser om dirigering och routning av e-posttrafik från konsumentanslutningar som blir kvar i föreskriften erbjuder en tillräcklig möjlighet att upptäcka och begränsa skräppost. Efter denna ändring finns det inte några hinder för att koppla SMTP-servrar till konsumentanslutningar då författningarna inte längre ålägger några begränsningsskyldigheter.

Bestämmelserna om upptäckt, filtrering och fränkoppling av skadlig trafik har omgrupperats under 6–8 §. Skyldigheterna omfattar nu att teleföretagen ska ha färdighet att upptäcka trafik som orsakar fara för kommunikationsnätets och -tjänstens informationssäkerhet och att spåra trafik som innehåller felaktiga källadresser.

Skyldigheter som gäller uppföljning av internetförbindelsetjänsternas funktion och kvalitet har tagits bort från denna föreskrift. Skyldigheterna har flyttats till föreskrift 58/2009 M.

Föreskriftens 9 § preciserar skyldigheten att behandla och registrera kränkningar av informationssäkerhet. En ny skyldighet är att teleföretagen ska föra statistik över de kränkningar som de har behandlat och de åtgärder som de har vidtagit. Paragrafen förutsätter dessutom att teleföretagen ska upprätthålla behöriga kontaktadresser till vilka det är möjligt att göra anmälningar om kränkningar av informationssäkerhet.

3 1 § TILLÄMPNINGSSOMRÅDE

Föreskriften tillämpas på produktion av internetförbindelsetjänster som tillhandahålls i allmänna kommunikationsnät samt på system, kommunikationsnät och kommunikationstjänster som ett teleföretag använder för dessa funktioner. Föreskriften tillämpas därför till exempel inte på e-posttjänster eller snabbmeddelandetjänster som tillhandahålls via internetförbindelsetjänsten. Föreskriften tillämpas på den IP-tjänst som behövs för genomförande av e-post- och snabbmeddelandetjänster.

Föreskriften tillämpas i tillämpliga delar för produktion av internetförbindelsetjänster hos både nätföretag och tjänsteföretag.

4 2 § DEFINITIONER

Här behandlas de definitioner som används i föreskriften. I föreskriften definieras inte samma termer som definieras i lag.

4.1 Internetförbindelsetjänst

Med *internetförbindelsetjänst* avses i denna föreskrift en kommunikationstjänst som gör det möjligt att koppla upp en förbindelse till internet och använda tjänster som internet erbjuder.

4.2 Kundanslutning

Med *kundanslutning* avses i denna föreskrift det logiska gränssnittet mellan ett kundnät och internetnät som är avsett för både konsument- och företagsbruk. Abonnenten till anslutningen blir en användare efter att ha blivit kopplad till det allmänna kommunikationsnätet och tjänsterna i det genom en kundanslutning.

Med gränssnitt mellan kundanslutningen och internetnätet avses i denna föreskrift det logiska gränssnitt med vilket man skiljer åt två skilda nät eller en enskild användare och ett enskilt nät. Tekniskt sett kan gränssnittet ligga exempelvis mellan kundnätet och nätföretagets nät samt mellan nätföretagets nät och tjänsteföretagets nät. Det logiska gränssnittet kan också ligga mellan kundens virtuella nät och det offentliga internetnätet.

En kundanslutning kan genomföras med hjälp av flera alternativa tekniker, såsom analog modemförbindelse, radionät, trådlöst lokalnät, kabelnät eller DSL.

Gränssnitt som hänför sig till genomförandet av en kundanslutning illustreras i följande schema.

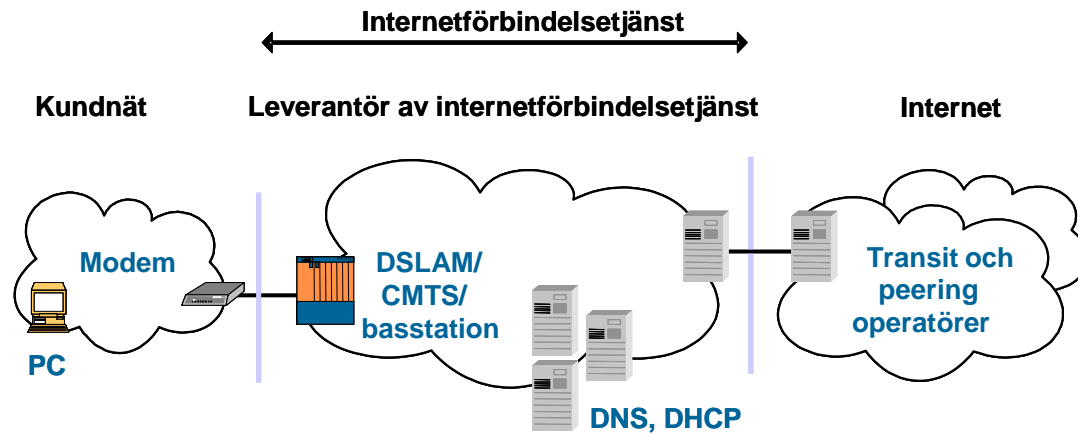


Bild 1. Exempel på gränssnitt till kundanslutningen.

4.3 Tjänster i en kundanslutning

Med *tjänster i en kundanslutning* avses i denna föreskrift tjänster som ett teleföretag tillhandahåller sina kunder via kundanslutningen för förmedling av internettrafik.

Tjänster som tillhandahålls genom en kundanslutning för förmedling av internettrafik är till exempel namntjänst (DNS), tjänst som används för tilldelning av internetadresser (DHCP), tjänst för förmedling av e-post (SMTP) samt www-proxytjänst.

4.4 Skadlig trafik

Med *skadlig trafik* avses sådan telekommunikation som kan äventyra kommunikationsnätets eller tjänstens informationssäkerhet. Trafik som orsakas av blockeringsattacker, skräppost och spridning av nätmaskar är exempel på skadlig trafik.

4.5 Filtrering

Med *filtrering* avses i denna föreskrift förhindrande eller begränsning av internettrafik i enlighet med i förväg specificerade regler.

Med filtrering kan avses att internettrafik som utgår från en kundanslutning och nyttjar förfalskade källadresser förkastas. Genom att jämföra adresserna med de adressrymder som beviljats kunden kan adresserna konstateras vara förfalskade.

Filtrering kan också innebära att kapacitet av en viss typ av internettrafik begränsas för en enskild anslutning. Filtrering kan också ske på basis av det tillämpningsprotokoll som använts i trafikeringen.

Det är möjligt att filtrera trafiken utan tjänsteanvändarens tillstånd, om åtgärderna behövs för att avvärja hot mot informationssäkerheten i kommunikationsnätet eller kommunikationstjänsten eller för att handha informationssäkerheten. Vid genomförandet av filtreringen ska teleföretaget utöver 5 kap. i lagen om dataskydd vid elektronisk kommunikation också ta hänsyn till de krav som bland annat ställs i kommunikationsmarknadslagen.

5 3 § KUNDANSLUTNINGARNAS INFORMATIONSSÄKERHET

5.1 Att skilja användarnas trafik från varandra

Ett teleföretag ska skilja kundanslutningarnas trafik från varandra så att användarna av de olika kundanslutningarna inte obehörigt kan följa med varandras trafik. Teleföretaget ska säkerställa att det inte är möjligt att obehörigen omdirigera trafik mellan anslutningarna.

Oberoende av vad som bestäms i 1 mom. kan teleföretaget tillhandahålla okrypterade WLAN-förbindelser utan att skilja trafiken i radiogränssnittet.

Motivering

Internetanslutningar som nyttjar delad kapacitet bland abonnenterna har exempelvis använts för 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 till exempel i stadsnät där tjänsten är öppen för alla som befinner sig inom nätets räckvidd.

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. Därför finns det en särskild avvikelse för okrypterade WLAN-förbindelser och teleföretaget kan tillhandahålla okrypterade WLAN-förbindelser utan att skilja åt trafiken i radiogränssnittet.

Tillämpning

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 trafikkratering. Abonnenternas trafik kan också skiljas åt med hjälp av portisoleringsegenskapen för DSLAM-koncentratorer eller switchar, i synnerhet då man använder en grupp-VLAN-identifierare.

Med WLAN-förbindelser avses förbindelser via trådlösa lokalnät i enlighet med IEEE-standard 802.11.

6 4 § INFORMATION

6.1 Information till kunden

Senast när kundanslutningen tas i bruk ska teleföretaget underrätta kunden om de allmänna informationssäkerhetsrisker och risker för enskilda anslutningstyper som hänför sig till användningen av anslutningen samt om de åtgärder som är tillgängliga för kunden för handhavandet av informationssäkerheten.

Motivering

Med allmän information om informationssäkerhet till kunder ökar teleföretaget kundernas medvetenhet om de allmänna risker som hänför sig till internetförbindelsernas och -tjänsternas informationssäkerhet. Det är möjligt att undvika en avsevärd del av de rapporterade problemen, om kunderna på ett behörigt sätt ser till att terminalutrustningen har ett grundläggande skydd och internettjänster används med beaktande av hot mot informationssäkerheten.

Om kunden skyddar sin terminalutrustning dåligt och använder internettjänster ovarsamt äventyras informationssäkerheten inte bara i kundens egen terminalutrustning utan också i tjänster som andra internetanvändare använder och i internettjänster som ett teleföretag tillhandahåller.

Det är också viktigt att kunderna kan skydda sig mot informationssäkerhetshot som berör en specifik anslutningstyp. Teleföretaget ska därför se till att kunden blir informerad om dessa hot samt om de informationssäkerhetsåtgärder som kunden kan vidta innan anslutningen kopplas.

Tillämpning

Information om allmänna informationssäkerhetsrisker

Beroende på tjänsten kan informationen ges till exempel när kunden beställer anslutningen eller senast när kunden börjar använda anslutningen. Det avgörande är att kunden får informationen innan han eller hon aktivt börjar använda anslutningen.

Teleföretaget kan uppfylla sin informationsskyldighet till exempel så att de nödvändiga uppgifterna fogas till avtalsdokumenten. Kunden kan också bli informerad på något annat sätt, om tjänsten som används möjliggör det. I så fall kan informationen till exempel ges på en inloggningssida då förbindelsen tas i bruk eller i samband med leveransen av ett elektronisk avtal. Allmän säkerhetsinformation på teleföretagets webbplats uppfyller inte de krav som ställs i paragrafen,

emedan kunden inte uttryckligen ombeds läsa den när anslutningen tas i bruk. Kunden kanske aldrig besöker den webbplatsen.

Kommunikationsverket upprätthåller en webbsida om de vanligaste informationssäkerhetshoten. Teleföretaget kan sköta kundinformationen också genom att be kunden besöka Kommunikationsverkets webbplats.

Huvudvikten i informationen ska gälla de åtgärder som kunden eller användaren av en kundanslutning kan vidta för att handha informationssäkerheten i sin egen terminalutrustning. Sådana är till exempel att kryptera trafiken, att skilja åt användarnas trafik, att ta i bruk en brandvägg innan datorn ansluts till nätet, att skaffa virusskydd och att uppdatera operativsystemet och andra program.

Information om informationssäkerhetsrisker för enskilda anslutningstyper

Med informationssäkerhetsrisker för enskilda anslutningstyper avses speciella risker som beror på det tekniska förverkligandet av anslutningen. Ett exempel är att tillhandahålla internetförbindelsetjänster med hjälp av en okrypterad WLAN-förbindelse. I sådana situationer ska teleföretaget underrätta kunden om de särskilda risker som kan förekomma då anslutningen används för konfidentiell kommunikation.

Teleföretaget är skyldigt att sköta sin informationsplikt också när det tillhandahåller sammanslutningsabonnenter anslutningar som sedan tillhandahålls sammanslutningsabbonenternas egna slutanvändare. Ett exempel på detta är telekommunikationsförbindelser som ett husbolag skaffar för sina invånare. Teleföretaget ska underrätta sina kunder om informationssäkerhetsrisker som hänför sig till fördelning av kapacitet.

6.2 Kundinformation om anslutningens tekniska begränsningar

Teleföretaget ska för kunden definiera och göra upp en beskrivning på de centrala och permanenta tekniska begränsningar som hänför sig till användningen av kundanslutningen. De kan gälla kommunikationsportar, -protokoll eller trafikvolym. Av beskrivningen ska också framgå de principer som tillämpas när det blir nödvändigt att ingripa i användningen av anslutningen eller tjänsterna som äventyrar kommunikationstjänsternas informationssäkerhet.

Motivering

Tekniska begränsningar som påverkar användningen av kundanslutningar är viktiga grundläggande egenskaper hos anslutningen. Begränsningarna inverkar bland annat på vilka informationssäkerhetsrisker som kunden själv bör förbereda sig på och vilka tjänster som kunden kan använda via anslutningen. Därför är det viktigt att beskriva begränsningarna på ett ändamålsenligt sätt.

Tillämpning

Med permanenta tekniska begränsningar avses begränsningar som specifikt definierats eller faktorer som beror på egenskaperna i operatörens nät vilka påverkar användningen av anslutningen. Sådana är till exempel:

- IP-protokollversioner som stöds
- telekommunikationsportar till vilka trafik förhindras eller begränsas
- eventuella begränsningar i applikationsprotokoll eller enskilda applikationer
- eventuell nätadressöversättning (NAT) som genomförs i anslutningsgränssnittet
- principerna för prioritering av trafik, t.ex. när en viss trafikvolym överskrids
- största tillåtna MTU-storleken, om den är mindre än 1500 byte.

Teleföretaget ska dessutom beskriva de principer som tillämpas när det blir nödvändigt att ingripa i användning av anslutningen eller tjänsterna som äventyrar kommunikationstjänsternas informationssäkerhet.

Beskrivningen av trafikbegränsningarna behöver inte vara så detaljerad att den i sig äventyrar informationssäkerheten hos teleföretagets tjänst till exempel genom att ge en alltför detaljerad bild

av de filtreringsmetoder som används. Beskrivningen kan också ges i samband med tjänstebeskrivningen eller på teleföretagets webbplats.

Tillfälliga tekniska begränsningar behöver inte beskrivas. Exempel på sådana är åtgärder som vidtas då teleföretaget måste utreda ett akut informationssäkerhetsläge.

Om teleföretaget inför nya begränsningar till användningen eller ändrar de befintliga begränsningarna under anslutningsavtalets giltighetstid, ska teleföretaget beakta det spelrum som avtalet tillåter. Om de nya begränsningarna kan antas vara en ensidig ändring av anslutningsavtalet, ska man iaktta de förfaringsätt som ges i lagstiftningen om ändring av avtal. Det finns tvingande bestämmelser om standardavtalsvillkor för konsumentkunder och ändringen av avtalet i kommunikationsmarknadslagen.

7 5 § DIRIGERING OCH ROUTNING AV E-POSTTRAFIK FRÅN KONSUMENTANSLUTNING

7.1 Förhindrande av obegränsad SMTP-trafik från konsumentanslutning

Ett teleföretag som tillhandahåller internetanslutningar måste förhindra obegränsad SMTP-trafik från konsumentanslutningar om det sker på annat sätt än via överenskomna servrar avsedda för utgående SMTP-trafik.

Motivering

Obegränsad SMTP-trafik (port 25) från en anslutning till internetnätet 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 begränsa mängden skräppost som de skadliga programmen producerar. Begränsningen påverkar inte användarnas kommunikationsmöjligheter, då det är möjligt att skicka e-post även via det teleföretags postserver som tillhandahåller internetanslutningen, med hjälp av autentiserad e-post (Mail Submission, RFC 4109 [9]) eller användargränssnitt för www-baserade e-posttjänster. Genom föreskriften bekräftas rekommenderad praxis för metoder för sändning av e-post som finns i IETF-dokument RFC 5068 [10].

Tillämpning

Med förhindrande av obegränsad SMTP-trafik avses blockering av trafik som går ut från cyberrymd avsedd för konsumentanslutningar 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 ha inverkan 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 4409 [9]. Detta gör det möjligt för kunder till teleföretaget som tillhandahåller internettjänster att också tryggt och autentiserat kommunicera med e-postsystem som en annan tjänsteleverantör förfogar över.

7.2 Tillåten SMTP-trafik från konsumentanslutning i speciella fall

Oberoende av vad som bestäms i 1 mom. kan teleföretaget 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. Teleföretaget ska också ha färdighet att snabbt reagera på störningar.

Motivering

Med tillåten obegränsad SMTP-trafik avses möjlighet till trafik som går ut från cyberrymd avsedd för teleföretagets konsumentanslutningar till mottagare utanför teleföretagets nät, genom kommunikationsport 25 som är reserverad för utgående SMTP-trafik.

Några 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.

Tillämpning

Teleföretaget ska underrätta abonnenten om de risker som hänför sig till öppen trafik. Teleföretaget ska också ha färdighet att snabbt reagera på störningar.

8 6 § UPPTÄCKT AV SKADLIG TRAFIK

8.1 Upptäckt av skadlig trafik

Ett teleföretag ska kontrollera och vid behov utreda händelserna i sitt eget kommunikationsnät för att upptäcka sådan trafik som äventyrar informationssäkerheten i kommunikationsnätet eller kommunikationstjänsten. Teleföretaget ska ha färdighet att spåra trafik som innehåller felaktiga källadresser.

Teleföretaget ska också utrusta sitt kommunikationsnät med en sådan upptäcktsförmåga som möjliggör de åtgärder som bestäms i 1 mom.

Motivering

Syftet med skyldigheten är att säkerställa att teleföretagen har tillräckliga förfaringsätt och system för att kunna upptäcka skadlig trafik och olika störningssituationer. Exempel på situationer som kräver upptäcktsförmåga är trafik till en viss kommunikationsport som ett snabbt spridande skadligt program orsakar, eller en blockeringsattack eller en störning i nättroutningen. Upptäckt av skadlig trafik mot teleföretagets kommunikationsnät eller upptäckt av skadliga händelser gör det möjligt för teleföretaget att handha nätets informationssäkerhet.

Trafik som innehåller felaktiga källadresser används generellt i blockeringsattacker. Syftet med utredningen av källan till sådan trafik är att det blir möjligt att begränsa eller avvärja de effekter som skadlig trafik orsakar tjänstens eller användarens informationssäkerhet.

Tillämpning

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 teleföretags kommunikationsnät kan man i allmänhet inte ha ett sådant system utan att nätets prestanda avsevärt påverkas. Insamlingen av uppgifterna kan då basera sig på trafikprov då man endast betraktar 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 t.ex. använda ett automatiskt system för hantering av trafikvolym eller exceptionella händelser i nätet, och systemet larmar om de förinställda gränsvärdena överskrids. För hantering av informationssäkerhetshändelser i nätet är det också möjligt att använda automatiska intrångsdetekteringssystem eller automatiska intrångsförhindrande system.

Teleföretaget ska ha handlingsmönster som det har gjort upp på förhand och förfaringsätt som det har övat på förhand vilka gör det möjligt att finna källan till skadlig trafik också om den skadliga trafiken innehåller felaktiga källadresser. Källan till skadlig trafik ska kunna identifieras utan dröjsmål i teleföretagets egna nät med en kundanslutnings noggrannhet. Om skyldigheter som gäller sammankopplingsgränssnitt bestäms i Kommunikationsverkets föreskrift 28 [6].

9 7 § FILTRERING AV SKADLIG TRAFIK

9.1 Processer och handlingsmönster för tillfällig filtrering av trafiken

Ett teleföretag ska ha processer och handlingsmönster enligt vilka trafiken temporärt filtreras i situationer som äventyrar informationssäkerheten i kommunikationsnätet eller kommunikationstjänsten. Teleföretaget ska ha teknisk färdighet att vidta dessa åtgärder.

Motivering

Teleföretaget ska ha färdiga processer och handlingsmönster för temporär filtrering av skadlig trafik, så att den kan filtreras bort från kommunikationsnätet så snabbt som möjligt. Teleföretaget ska se till att processerna och handlingsmönstren hålls uppdaterade.

Med hjälp av filtrering är det möjligt att exempelvis begränsa effekten av sådana blockeringsattacker 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.

Tillämpning

I en situation som äventyrar kommunikationsnätets eller -tjänstens informationssäkerhet kan teleföretaget bli tvunget att vidta tillfälliga åtgärder för att blockera trafik via vederbörande kommunikationsport till och från kundanslutningar eller för att begränsa trafik från kundanslutningar 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 internetjänsteleverantörens nätelement stöder begränsning av trafikvolymerna på basis av enskilda protokoll, adresser, portar och nätaccesser. Begränsningar ska kunna genomföras så att nätets tillgänglighet inte äventyras i onödan. Tekniska färdigheter förutsätter också att teleföretagets nätoperatörscentral har förmåga att starta nödvändiga filtreringsåtgärder.

Nätelement som begränsar trafikvolymerna ska vid behov kunna lagra ändamålsenliga händelseuppgifter om filtrering. Sådana uppgifter kan vara käll- och måladresser, käll- och målportar samt information om den åtgärd som gjordes. Vid bedömning av ändamålsenlighet ska man exempelvis beakta tillräcklig noggrannhet för provtagning. Händelseuppgifterna är nödvändiga för t.ex. utredning av problem och nätattacker eller för identifiering. Nätelementet ska även möjliggöra en aktuell analys av händelseuppgifterna. Händelseuppgifterna ska tidsstämplas och tidsinställningen ska nyttja en centraliserad rättidig tidskälla.

9.2 Filtrering av trafik som innehåller felaktiga källadresser

Teleföretaget ska filtrera sådan trafik från en kundanslutning till kommunikationsnätet vars källadress inte är anvisad vederbörande kundanslutning. Teleföretaget ska genomföra filtreringen i det nätelement som befinner sig närmast kundgränssnittet och där det tekniskt är mest ändamålsenligt att göra filtreringen.

Motivering

I distribuerade blockeringsattacker (DDoS) använder man ofta förfalskade källadresser för kommunikation för att göra det svårare att finna 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 speciella ändamål.

Syftet med kraven är att begränsa problem som orsakas av attacker som begås med förfalskade IP-källadresser i nätet.

Tillämpning

För att blockera trafik som utnyttjar förfalskade källadresser måste ett teleföretag som tillhandahåller kundanslutningar filtrera sådan trafik från en kundanslutning till kommunikationsnätet vars källadress inte är anvisad vederbörande kundanslutning. Teleföretaget ska vid behov kunna identifiera den kundanslutning vars trafik mot nätet har felaktiga källadresser.

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

Teleföretaget som tillhandahåller kundanslutningar bör även filtrera sådan trafik från kommunikationsnätet till kundanslutningen där källadressen ingår i den adressrymd som vederbörande anslutning hör till. (RFC 3013, punkterna 4.3 och 4.4 samt RFC 3704 för multihoming-nätens del).

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

9.3 Identifiering av en användare

En lindrigare åtgärd än filtrering av trafik är att teleföretaget kontaktar kunden för att utreda situationen som äventyrar informationssäkerheten.

Motivering

Enligt lagen om dataskydd vid elektronisk kommunikation kan teleföretaget 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. Enligt Kommunikationsverkets tolkning är det klart att 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. Om användaren eller den som representerar användaren inte kan nås eller hotet annars inte kan elimineras, kan teleföretaget vidta åtgärder för att begränsa trafiken.

Tillämpning

Teleföretagets rätt att behandla identifieringsuppgifter för identifiering av en kund beskrivs under avsnitt 1.3.1. Åtgärderna ska utföras omsorgsfullt och så att åtgärderna står i rätt proportion till den störning som ska avväjas. Åtgärderna får inte begränsa yttrandefriheten, skyddet av konfidentiella meddelanden eller integritetsskyddet mer än nödvändigt med tanke på säkerställandet av möjligheterna att uppnå målet för behandlingen av identifieringsuppgifterna.

9.4 Adress- och ruttfiltrering

Om ett teleföretag för filtrering av trafik eller routningsinformation använder filtreringsregler som baserar sig på adressrymder som är reserverade för speciella ändamål eller som inte är i bruk, ska teleföretaget se till att filtreringsreglerna är uppdaterade.

Motivering

Vid användning av filtreringslistor ska man fästa särskild uppmärksamhet vid att reglerna för filtrering hålls uppdaterade, så att föråldrade regler inte begränsar ändamålsenlig användning av redan beviljade IP-nätresurser. Teleföretaget ska regelbundet kontrollera att filtreringsreglerna är uppdaterade.

Tillämpning

Filtrering kan göras på basis av ruttannonser för att hindra kapning av icke-använda adressrymder samt på basis av källadresser för att begränsa blockeringsattacker. Eftersom det i blockeringsattacker regelbundet också används rent förfalskade källadresser som dock routas, är det skäl att grundligt överväga behovet av adressfiltrering och se över uppdateringsmekanismerna.

Vid filtrering av routningsinformation eller trafik ska teleföretaget se till att filtreringslistan är uppdaterad för att undvika till exempel filtrering av en adressrymd som nyligen tagits i bruk.

Adressrymder som eventuellt kan filtreras kan vara så kallade bogon-prefix som är reserverade för privat bruk (RFC 1918) eller för speciella ändamål och som inte är avsedda för öppen användning i internettätet. Andra motsvarande adressrymder kan vara nät som IANA (Internet Assigned Numbers Authority) eller lokala internetadressregister ännu inte har beviljat.

Vid bogon-filtrering kan man använda BGP-routningsinformation (Border Gateway Protocol) som tillförlitliga instanser tillhandahåller och där ändringar i bruket av adressrymder centraliserat överförs i de regler som används för filtreringen.

Utrustning som är försedd med default-bogon listor ska inte användas, eftersom de är föråldrade.

9.5 Genomförande av filtreringsåtgärder

Enligt 20 § 4 mom. i lagen om dataskydd vid elektronisk kommunikation ska filtreringsåtgärder utföras omsorgsfullt och de ska stå i rätt proportion till den störning som ska avväjas. Åtgärderna får inte begränsa yttrandefriheten, skyddet av konfidentiella meddelanden eller integritetsskyddet mer än nödvändigt med tanke på säkerställandet av möjligheterna att uppnå målen för åtgärden. Åtgärderna ska avbrytas, om det inte längre finns i lag nämnda förutsättningar för att vidta dem.

10 8 § FRÅNKOPPLING AV ANSLUTNINGEN

10.1 Frånkoppling av kundanslutningar

Teleföretaget ska koppla ur en kundanslutning eller en tjänst från det allmänna kommunikationsnätet om kommunikationstjänstens informationssäkerhet väsentligen äventyras av orsaker som beror på anslutningen.

Motivering

Kundanslutningens funktion kan väsentligt äventyra kommunikationstjänstens informationssäkerhet till exempel i situationer där ett system som är kopplat till anslutningen har drabbats av ett skadligt program och sänder stora mängder skräppost eller skadliga program. Smittad terminalutrustning som ansluts till teleföretagets nät äventyrar alltid informationssäkerheten hos teleföretagets tjänster i den mån att teleföretaget har rätt att vidta åtgärder för att eliminera hotet som den smittade terminalutrustningen orsakar.

Tillämpning

Att en tjänst vid en kundanslutning kopplas från det allmänna kommunikationsnätet avser i denna föreskrift exempelvis tillfällig avstängning av de kommunikationsportar till vilka sådan 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 en blockeringsattack och därför mottar exceptionellt stora trafikvolymer i en viss situation.

Vid handhavandet av informationssäkerheten och i frånkopplingsituationer är det skäl att fästa uppmärksamhet vid att identifieringsuppgifter får behandlas endast då det är frågan om hot mot eller kränkningar av informationssäkerhet i kommunikationsnät och kommunikationstjänster. Teleföretaget har alltså inte rätt att behandla identifieringsuppgifter till exempel för att hindra användningen av anslutningen vid brott som inte äventyrar tjänstens informationssäkerhet. Ett undantag är dock förberedelse till betalningsmedelsbedrägerier som avses i 20 § 1 mom. 3 punkten i lagen om dataskydd vid elektronisk kommunikation.

10.2 Anvisningar för frånkopplingsprocessen

Frånkopplingen och återkopplingen ska göras enligt de processer och instruktioner som teleföretaget i förväg har specificerat. I samband med åtgärderna kan speciella förhållanden som beror på anslutningstyp och hotets allvar beaktas.

Motivering

Frånkoppling av anslutningen gör att kunden inte kan använda anslutningen i fråga. Det ska därför finnas detaljerade planer och instruktioner för frånkopplingsprocessen. Ändamålsenlig registrering av de åtgärder som vidtas och därtill relaterad kommunikation säkerställer också teleföretagets och kundernas rättskydd.

Tillämpning

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

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

Instruktionerna om frånkopplingen ska innehålla nödvändiga förfaringsätt för att återinkoppla kundanslutningen till kommunikationsnätet, när teleföretaget har konstaterat att informations säkerhetshotet 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.

Tjänste- och nätoperatören kommer sinsemellan överens om de principer som hänför sig till det praktiska genomförandet av frånkopplingen. Båda parterna ska ha möjlighet att vidta behövliga åtgärder för att handha informations säkerheten i sin tjänst eller i sitt nät. Den andra parten ska underrättas om från- och återinkopplingen utan dröjsmål.

I samband med åtgärderna kan speciella förhållanden som beror på anslutningstyp beaktas. Då det t.ex. gäller anslutningstyper för tjänsteleverantörer kan man komma överens om sådana handlingsmönster vid störningar att olägenheterna vid tillhandahållandet av tjänster blir så små som möjligt. Om det t.ex. finns ett informations säkerhetsproblem i mobilabonnemangets mobildatatjänst kan teleföretaget endast hindra användningen av mobildatatjänsten tills informations säkerhetsproblemet är utrett.

Om kundanslutningarna omfattas av automatisk kontroll, sker frånkopplingen av kundanslutningarna eller vissa tjänster i kundanslutningen normalt vid behov automatiskt för t.ex. 30 minuter utan åtgärder från operatörens sida när gränsvärdena för skadlig trafik har överskridits. När anslutningen är frånkopplad kan kundens trafik styras till en tjänst där kunden underrättas om orsaken till frånkopplingen och om eventuella åtgärder som kunden kan vidta för att avhjälpa felet. Dessutom kan kunden ha möjlighet att besöka behövliga sidor till exempel för att installera viruskydd och uppdatera operativsystemets programvara. Detta förfarande minskar behovet av en mera varaktig frånkoppling.

Vid användning av automatiska system för stängning och öppning av kundanslutningar i syfte att handha informations säkerheten av tjänsten, ska kunden underrättas om de principer som hänför sig till den tillfälliga stängningen och öppningen av anslutningen.

11 9 § BEHANDLING OCH STATISTIKFÖRING AV KRÄNKNINGAR AV INFORMATIONSSÄKERHET

11.1 Kontaktadresser för anmälning av kränkningar av informations säkerhet

Ett teleföretag ska se till att det har kontaktadresser till vilka det är möjligt att anmäla kränkningar av informations säkerhet. Kontaktadresserna ska offentliggöras på teleföretagets webbplats i ett lämpligt avsnitt.

Motivering

Ändamålsenliga kontaktadresser som är enkelt tillgängliga gör det lättare för teleföretaget att behandla informationssäkerhetskränkningar. Uppgifter om en kränkning kan direkt styras till dem som behandlar sådana fall. Kontaktadresser behövs också för registrering av abuse- och irt-kontaktuppgifterna i den lokala internetregistratorstjänsten.

Tillämpning

Minimivån kan antas vara en e-postadress och meddelanden som sänds till denna adress styrs till dem som behandlar informationssäkerhetskränkningar i teleföretaget. E-postadressen har ofta formen abuse@teleyrityksen_verkkotunnus.

Information om kontaktadresserna ska publiceras på teleföretagets webbsidor på en lämplig plats.

Teleföretaget ska också beakta de skyldigheter som ges i 4 § i Kommunikationsverkets föreskrift 28 H/2010 M samt de tillämpningsanvisningar som ges i avsnitt 6.3 i dokumentet MPS 28 vad gäller dokumentation av IP-adressblock med behöriga abuse- och irt-kontaktuppgifter i databasen för internetadressregistret.

11.1.1 Rekommendationer

Det rekommenderas att anvisningar som hänför sig till informationssäkerhetskränkningar och informationssäkerhet samt kontaktuppgifter publiceras på teleföretagets www-tjänst som en särskild sida som även innehåller sådana anvisningar som kunden kan följa för att utreda kränkningar på eget initiativ.

Det rekommenderas att kontaktuppgifterna också publiceras på engelska.

11.2 Behandling av kränkningar av informationssäkerhet

Teleföretaget ska på ett behörigt sätt behandla och registrera de kränkningar av informationssäkerhet som det har fått beträffande teleföretagets tjänster och kunder.

Motivering

För att ta hand om informationssäkerheten för sina tjänster ska teleföretaget på ett effektivt och ändamålsenligt sätt behandla de kränkningar av informationssäkerhet mot teleföretagens tjänster och kunder som det har fått veta om. Om teleföretaget försummar att behandla händelserna äventyras informationssäkerheten hos teleföretagets tjänster och kunder och indirekt också hos användare av andra kommunikationsnät.

Teleföretaget ska registrera alla kränkningar som det behandlar i syfte att säkerställa rättskyddet för teleföretagens kunder och en behörig utredningsprocess.

Tillämpning

Teleföretaget ska bestämma vem som ansvarar för kommunikationsnätets och -tjänsternas informationssäkerhet och tar emot anmälningar om händelser som kan äventyra informationssäkerheten för att utreda dem. Teleföretaget ska kontrollera anmälningarnas riktighet på ett ändamålsenligt sätt.

Med behörig behandling av kränkningar av informationssäkerhet avses, beroende på kränkningens art, till exempel utredning av kränkningen och minimering av eventuella skador. Om kränkningen inte riktar sig mot teleföretagets egen kund eller om teleföretaget annars inte kan utreda kränkningen med egna medel, kan ärendet utredas av en aktör som kan inverka på kränkningen. En sådan aktör kan var ett annat teleföretag eller en CERT-aktör, i Finland Kommunikationsverkets CERT-FI.

Med behörig registrering avses registrering av alla informationssäkerhetskränkningar som teleföretaget behandlar. Teleföretaget ska dessutom registrera alla de åtgärder som det vidtar för att utreda fallen.

11.3 Statistikföring av anmälningar

Teleföretaget ska föra statistik över de kränkningar som det har behandlat och de åtgärder som det har vidtagit uppdelade efter typ. Av statistiken ska åtminstone framgå följande uppgifter:

- *det totala antalet kränkningar av informationssäkerhet som teleföretaget har behandlat*
- *antalet fortsatta åtgärder som kränkningarna av informationssäkerhet har orsakat, uppdelade efter typ av åtgärd*
- *antalet abonnenter som de fortsatta åtgärderna har gällt, uppdelade efter kundgrupp.*

Motivering

För att kunna övervaka huruvida teleföretagets åtgärder är tillräckliga och ändamålsenliga ska det föra statistik över de kränkningar som det har behandlat och de åtgärder som teleföretaget har vidtagit för att utreda dem.

Kommunikationsverket ber regelbundet teleföretagen att uppge uppgifter som är nödvändiga för att verket ska kunna utföra sin övervakningsuppgift. Kommunikationsverkets rätt att få information baserar sig på 33 § 1 mom. i lagen om dataskydd vid elektronisk kommunikation. Där bestäms att utan hinder av sekretessbestämmelserna eller av andra begränsningar som gäller utlämnande av uppgifter har Kommunikationsverket rätt att av teleföretag samt av dem som verkar för dessa få sådana uppgifter om deras i denna lag avsedda verksamhet som är nödvändiga för att Kommunikationsverket ska kunna utföra sina i denna lag föreskrivna uppgifter.

Statistikföringen betjänar också uppföljningen av teleföretagets interna processer med avseende på processernas funktion och informationssäkerhetsläget i nätet.

Tillämpning

Teleföretaget ska göra upp en statistik över informationssäkerhetskränkningar som det har behandlat så att av statistiken framgår:

- det totala antalet kränkningar
- antalet fortsatta åtgärder som kränkningarna har orsakat
 - kontakt med kunden
 - filtrering av trafik
 - frånkoppling av anslutningen eller tjänsten
 - överföring till en annan aktör
 - onödig anmälan, inga åtgärder
- antalet abonnenter som ovan nämnda åtgärder har gällt, uppdelade ändamålsenligt efter typ av anslutning.

Av de kränkningar som teleföretaget själv har upptäckt statistikförs de fall som har samband med teleföretagets kundanslutningar och tjänster.

Statistikperioden är ett kalenderår.

De uppgifter som teleföretagen tillställer Kommunikationsverket är på basis av lagen om offentlighet i myndigheternas verksamhet (621/1999) sekretessbelagda.

Rekommendation

Statistiken kan vara mera detaljerad än vad som beskrivs ovan. Kränkningar av informationssäkerhet som teleföretaget behandlar kan också statistikföras på basis av observerat problem t.ex. enligt följande uppdelning:

- Spridning av skräppost
- System som använts för blockeringsattack
- Upptäckt av olagligt bruk av ett system som är kopplat till kundanslutningen / dataintrång (t.ex. ändring av innehållet på en www-server)
- Upptäckt av ett skadligt program i ett system som är kopplat till anslutningen
- Kommandoserver för botnät

- Övriga informationssäkerhetsproblem.

12 10 § IKRAFTTRÄDANDE OCH ÖVERGÅNGSBESTÄMMELSER

Denna föreskrift träder i kraft den 1 april 2011 och gäller tills vidare. Genom föreskriften upphävs Kommunikationsverkets föreskrift 13 A/2008 M av den 19 september 2008 om Internetförbindelsetjänsternas informationssäkerhet och funktionsduglighet. Föreskriftens 9 § 3 mom. som gäller teleföretagens skyldighet att föra statistik träder i kraft den 1 januari 2012.

Motivering

Föreskriften träder i kraft samtidigt som föreskrift 28 H/2010 M. Skyldigheten att föra statistik, som finns i 9 § 3 mom. kan förutsätta förändringar i teleföretagens processer. Därför bestäms att skyldigheten att föra statistik börjar i början av 2012.

13 REFERENSLISTA

[1] Lagen om dataskydd vid elektronisk kommunikation (516/2004 jämte ändringar), uppdaterad version:

<http://www.finlex.fi/sv/laki/ajantasa/2004/20040516>

[2] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktivet om integritet och elektronisk kommunikation) (viestinnän tietosuojadirektiivi)

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:SV:NOT>

[3] Kommunikationsmarknadslagen (393/2003 jämte ändringar), uppdaterad version:

<http://www.finlex.fi/sv/laki/ajantasa/2003/20030393>

[4] Kommunikationsverkets föreskrift 9 D/2009 M om skyldighet att anmäla kränkningar av informationssäkerhet i allmän televerksamhet

<http://www.ficora.fi/attachments/ruotsiav/5m3u5L7aS/Kommunikationsverket09D2009M.pdf>

[5] Kommunikationsverkets föreskrift 11 A/2008 M om e-posttjänsternas informationssäkerhet och funktionsduglighet

<http://www.ficora.fi/attachments/ruotsiav/5AWNeO3Pw/Kommunikationsverket11A2008M.pdf>

[6] Kommunikationsverkets föreskrift 28 H/2010 M om interoperabilitet av kommunikationsnät och kommunikationstjänster, <http://www.ficora.fi/attachments/ruotsiav/5uSL7CR8M/M28H2010SV.pdf>

[7] Kommunikationsverkets föreskrift 47 C/2009 M om hantering av teleföretagens informationssäkerhet

<http://www.ficora.fi/attachments/ruotsiav/5jr9WfPYP/Kommunikationsverket47C2009M.pdf>

[8] Kommunikationsverkets föreskrift 57/2009 M om underhåll av kommunikationsnät och -tjänster samt om förfarande vid fel och störningar

<http://www.ficora.fi/attachments/ruotsiav/5kflA59Nj/Kommunikationsverket572009M.pdf>

[9] Internet Engineering Task Force (IETF) Request for Comments 4409: Message Submission for Mail

<http://tools.ietf.org/pdf/rfc4409.pdf>

[10] Internet Engineering Task Force (IETF) Request for Comments 5068: Email Submission Operations: Access and Accountability Requirements - BCP 134

<http://tools.ietf.org/pdf/rfc5068.pdf>

