

**MOTIVERING TILL OCH TILLÄMPNING AV
FÖRESKRIFT 11**

**OM E-POSTTJÄNSTERNAS
INFORMATIONSSÄKERHET OCH
FUNKTIONSDUGLIGHET**

Innehåll

1	LAGSTIFTNING	3
1.1	RÄTTSGRUND	3
1.2	ANDRA RELATERADE BESTÄMMELSER	4
2	SYFTET MED FÖRESKRIFTEN OCH ÄNDRINGSHISTORIA.....	4
2.1	SYFTET MED FÖRESKRIFTEN	4
2.2	CENTRALA ÄNDRINGAR OCH ÄNDRINGSHISTORIA	5
3	MOTIVERING TILL ENSKILDA PARAGRAFER OCH ANVISNINGAR FÖR TILLÄMPNING	5
3.1	1 § TILLÄMPNINGSSOMRÅDE.....	5
3.2	2 § DEFINITIONER.....	5
3.2.1	<i>E-posttjänst.....</i>	6
3.2.2	<i>Tjänst för förmedling av e-post.....</i>	7
3.2.3	<i>Sekundär tjänst för förmedling av e-post.....</i>	7
3.2.4	<i>Öppen proxyserver för e-post.....</i>	7
3.2.5	<i>Skadlig e-posttrafik.....</i>	7
3.2.6	<i>Filtrering</i>	7
3.3	3 § ÖPPNA PROXYSERVERAR FÖR E-POST	8
3.4	4 § HANTERING AV INKOMMANDE E-POSTTRAFIK	8
3.4.1	<i>Identifiering av skadlig e-posttrafik.....</i>	8
3.4.2	<i>Filtrering och märkning av e-posttrafik</i>	12
3.4.3	<i>Information om filtreringsprinciper för inkommande e-posttrafik</i>	13
3.5	5 § HANTERING AV UTGÅENDE E-POSTTRAFIK.....	13
3.6	6 § FÖRBINDELSE MELLAN KUND OCH E-POSTSERVER	14
3.7	7 § UPPFÖLJNING AV E-POSTTJÄNSTERNAS FUNKTIONSDUGLIGHET OCH KVALITET.....	15
3.8	8 § ADMINISTRERING AV E-POSTADRESSER	16
3.8.1	<i>Beskrivning av administrering av e-postadresser för kunder.....</i>	16
3.8.2	<i>Överlåtelse av e-postadress som blivit ledig</i>	17
3.8.3	<i>Administrering av problemsituationer med vilseledande e-postadresser.....</i>	17
3.9	9 § E-POSTTJÄNSTELEVERANTÖRENS KONTAKTUPPGIFTER	17
3.10	10 § IKRAFTTRÄDANDE OCH ÖVERGÅNGSBESTÄMMELSER	18
4	ÖVRIGA REKOMMENDATIONER	18
4.1.1	<i>Skydd av förbindelser mellan servrar.....</i>	18
5	REFERENSLISTA.....	18
6	FÖRKORTNINGAR.....	19

1 LAGSTIFTNING

Syftet med detta kapitel är att ge användaren av föreskriften en helhetsbild av de författningar som utgör grunden för föreskriften. Dessutom ges andra väsentliga författningar som har samband med innehållet.

1.1 Rättsgrund

Kommunikationsverkets föreskrift baserar sig på 128 och 129 § i kommunikationsmarknadslagen [1] samt 19 och 20 § i lagen om dataskydd vid elektronisk kommunikation (dataskyddslagen) [2]. Kommunikationsmarknadslagen som trädde i kraft den 25 juli 2003 verkställde för sin del EG:s direktiv om *elektronisk kommunikation*, dvs. ramdirektivet [3], auktorisationsdirektivet [4], tillträdesdirektivet [5] och direktivet om samhällsomsfattande tjänster [6] vilka godkändes i februari 2002. Dataskyddslagen som trädde i kraft 1.9.2004 verkställde för sin del EG:s direktiv om *dataskydd vid elektronisk kommunikation* [7] som godkändes i februari 2002.

Kommunikationsverket kan, med stöd av 19 § 4 mom. i dataskyddslagen ge ett teleföretag närmare föreskrifter om ovan i 1-3 mom. avsett dataskydd för tjänster. Enligt 1 mom. i paragrafen ska ett teleföretag handha dataskyddet för sina tjänster. På basis av 2 mom. gäller skyldigheten att handha dataskydd också den behandling av uppgifter, som behövs för fullgörandet av lagringsskyldigheten, som föreskrivs i lagen. Enligt 3 mom. är ett teleföretag gentemot abonnenterna och användarna ansvarigt för det dataskydd som avses i 1 och 2 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 20 § i dataskyddslagen ge ett teleföretag närmare föreskrifter om det tekniska förfarandet för att avvärja i denna paragraf avsedda kränkningar av tjänstens dataskydd samt för att eliminera störningar av dataskyddet. Enligt paragrafen har ett teleföretag och den som tillhandahåller mervärdestjänster rätt att vidta nödvändiga åtgärder för att säkra i 19 § avsett dataskydd.

Föreskriften gäller de krav som ställs i 128 § 1, 4, 5, 7 och 12 punkten i kommunikationsmarknadslagen där det bestäms att allmänna kommunikationsnät och kommunikationstjänster samt kommunikationsnät och kommunikationstjänster som ansluts till dem skall planeras, byggas och underhållas så att:

- 1) telekommunikationens tekniska standard är god,
- 4) användarnas eller andra personers datasekretess, dataskydd eller andra rättigheter inte äventyras,
- 5) användarnas eller andra personers hälsa eller egendom inte äventyras,
- 7) de är kompatibla och vid behov kan anslutas till ett annat kommunikationsnät,
- 12) teleföretaget även annars förmår fullgöra sina skyldigheter eller skyldigheter som ålagts företaget med stöd av denna lag.

I denna föreskrift preciseras ovan i 128 § nämnda tekniska krav utifrån 129 §, 2-5, 10, 15-16 och 20-21 punkten i lagen, enligt vilka Kommunikationsverkets föreskrifter kan gälla

- 2) kommunikationsnätets konstruktion,
- 3) prestanda i kommunikationsnät och kommunikationstjänster,
- 4) sammankoppling, kompatibilitet och signalering,
- 5) tekniska egenskaper hos anslutningspunkter i kommunikationsnätet,
- 10) säkerhet och störningsfrihet i kommunikationsnät,
- 15) tjänster som tillhandahålls användarna,
- 16) underhåll och uppföljning av prestanda samt nätverksadministration,
- 20) standarder som ska iakttas,
- 21) andra härmed jämförbara tekniska krav på kommunikationsnät eller kommunikationstjänster.

1.2 Andra relaterade bestämmelser

I detta avsnitt beskrivs Kommunikationsverkets andra föreskrifter som har samband med denna föreskrift. Syftet med avsnittet är att ge föreskriftens användare en bättre möjlighet att skapa sig en helhetsbild av de skyldigheter som gäller kommunikationsnät och kommunikationstjänster.

Föreskrift 9 om skyldighet att anmäla kränkningar av informationssäkerhet samt fel och störningar i allmän televerksamhet [8]. Föreskriften tillämpas på teleföretagens allmänna televerksamhet och på teleutrustningar som används i den. Föreskriften tillämpas också på televerksamhet i myndighetsnät och på utrustningar som används i dem.

Föreskrift 13 om Internetförbindelsetjänsternas informationssäkerhet och funktionsduglighet [9]. Föreskriften tillämpas på produktion av Internetförbindelsetjänster som tillhandahålls i allmänna kommunikationsnät samt på system, kommunikationsnät och kommunikationstjänster som ett teleföretag använder för dessa funktioner. Med Internetförbindelsetjänster avses i föreskriften förmedling av Internettrafik. Föreskriften tillämpas i tillämpliga delar också på produktion av Internetförbindelsetjänster i både nätföretag och tjänsteföretag.

Föreskrift 47 om informationssäkerhet hos teleföretag [10]. Föreskriften tillämpas på verksamhet som gäller genomförande av teleföretags allmänna kommunikationstjänster samt på de system, kommunikationsnät och kommunikationstjänster som teleföretagen använder för allmän televerksamhet och fastställer hur teleföretagen ska sköta ärenden relaterade till informationssäkerhet.

Föreskrift 53 om skyldighet att lagra identifieringsuppgifter [11]. I föreskriften bestäms om skyldighet för vissa teleföretag att lagra identifieringsuppgifter. Föreskriften ålägger inte ett teleföretag skyldighet att lagra någon ny information, utan avsikten är enbart att förlänga arkiveringstiden för den information teleföretagen redan nu lagrar för eget behov.

Föreskrift 54 om säkerställande av kommunikationsnät och kommunikationstjänster [12]. Syftet med föreskriften är att garantera funktionssäkerheten hos kommunikationsnät och kommunikationstjänster, dataskydd och informationssäkerhet under normala förhållanden, vid störningar under normala förhållanden och under undantagsförhållanden. Därför ålägger föreskriften teleföretagen minimikrav för bl.a. säkerställande av effektmatning för utrustningar för kommunikationsnät och -tjänster, fysiskt skydd av utrustningar och säkerställande av förbindelserna och utrustningarna.

Listan motsvarar läget vid den tidpunkt då detta dokument publicerades. Alla Kommunikationsverkets föreskrifter har publicerats på ämbetsverkets Internetsidor under adressen www.ficora.fi.

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 ändringar som gjorts i skyldigheter och rekommendationer före föreskriften.

2.1 Syftet med föreskriften

Syftet med föreskriften är att ålägga leverantörerna av e-posttjänster minimikrav för att säkerställa kommunikationstjänstens informationssäkerhet och funktionsduglighet.

Syftet med föreskriften är att säkerställa att konsumenterna har en fungerande e-posttjänst. Det är svårt för konsumenterna att bedöma kommunikationstjänstens informationssäkerhet och funktionsduglighet. Emedan det knappast finns någon möjlighet alls för konsumenterna att påverka kommunikationstjänsternas funktionsduglighet, bör e-posttjänsteleverantörerna via föreskrift åläggas minimikrav för de väsentliga tekniska egenskaperna för e-posttjänsten.

E-posttjänstens betydelse har också ökat i samhället som helhet. Därför ålägger föreskriften tjänsteleverantörerna krav på hantering av e-posttrafik, administrering av e-postserverar och -adresser samt uppföljning av tjänstekvalitet.

2.2 Centrala ändringar och ändringshistoria

I nuvarande version av föreskriften har e-posttjänsteleverantörens och Internetförbindelseleverantörens roll och uppgifter skilts åt beträffande e-posttjänsten. Denna föreskrift koncentrerar sig på e-posttjänsteleverantörens skyldigheter och uppgifter. Kraven på och rekommendationerna för de tjänsteleverantörer som erbjuder Internetförbindelsetjänster eller -anslutningar har överförts till föreskrift 13 (föreskrift om Internetförbindelsetjänsternas informationssäkerhet och funktionsduglighet).

Paragrafindelningen i föreskriften har förnyats. De krav som gäller en e-posttjänsteleverantör som i föregående föreskrift behandlas i 5 § (dirigering och routning av e-posttrafik till konsumentabonnemang), i 6 § (dirigering och routning av e-posttrafik från konsumentabonnemang) och i 7 § (upptäckt och filtrering av trafik med skadliga program) har i denna föreskrift samlats under två paragrafer (4 §, hantering av inkommande e-posttrafik och 5 §, hantering av utgående e-posttrafik). Avsikten med ändringen är att förtydliga innehållet och helheten i föreskriften.

Enligt 6 § i föreskriften har leverantören av e-posttjänster ålagts skyldighet att som primär förbindelse erbjuda en skyddad förbindelse mellan kunden och e-postlådan samt mellan kunden och e-postservern för utgående trafik.

En annan nyhet är administrering av e-postadresser, som hänvisas till i föreskriftens 8 §. Syftet med paragrafen är att harmonisera tjänsteleverantörernas olika praxis för administrering av e-postadresser samt ålägga tjänsteleverantörerna att informera konsumenterna om principerna för hur e-postadresserna administreras. Skyldigheten att säkerställa e-posttjänsternas funktionsduglighet har placerats under andra paragrafer och föreskriften om drift och underhåll av kommunikationsnät, som förnyas.

3 MOTIVERING TILL ENSKILDA PARAGRAFER OCH ANVISNINGAR FÖR TILLÄMPNING

Detta kapitel behandlar motiveringen till enskilda paragrafer samt rekommendationer för tillämpning av dem.

3.1 1 § Tillämpningsområde

Föreskriftens tillämpningsområde är att erbjuda konsument- och företagskunder sändnings-, förmedlings- och mottagningstjänster för e-postmeddelanden som tillhandahålls i allmänna kommunikationsnät, samt system som används för dessa funktioner. Föreskriften tillämpas på erbjudande av e-postmeddelanden oberoende av verksamhetens form. Föreskriften lämpar sig sålunda också t.ex. för en tjänst som erbjuds ett offentligt samfund eller en förenings alla intresserade användare av tjänsten. Föreskriften tillämpas dock inte på e-posttjänster som erbjuds en begränsad användargrupp, såsom e-posttjänster som ett företag eller en kommun erbjuder sina anställda.

Föreskriften tillämpas också på tjänster för omdirigering av meddelanden som räknas som förmedlingstjänster. Paragraferna 5 och 6 i föreskriften tillämpas ändå inte på dylika tjänster.

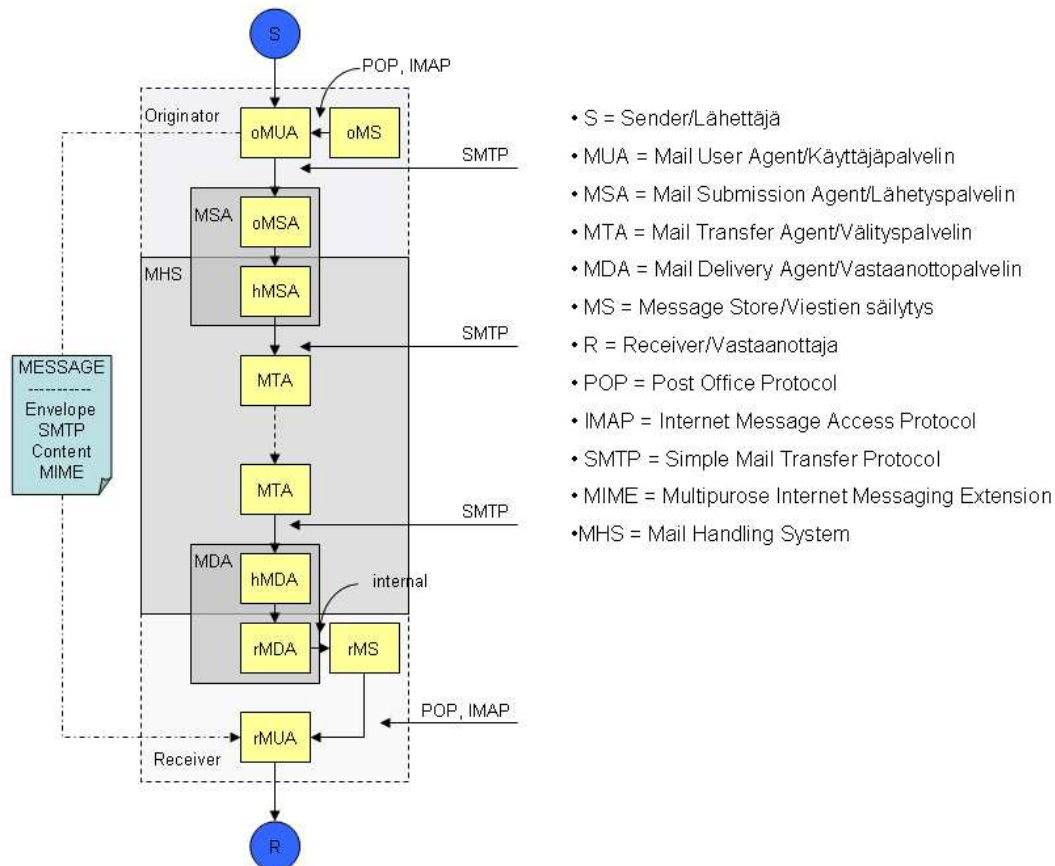
E-posttjänst och förmedling av e-postmeddelanden definieras närmare i avsnitt 3.2. Definitioner (avsnitten 3. 2.1, 3.2.2 och 3.2.3).

3.2 2 § Definitioner

Detta stycke behandlar de definitioner som används i föreskriften.

3.2.1 E-posttjänst

Med e-posttjänst avses i denna föreskrift en tjänst för sändning, förmedling eller mottagning av e-postmeddelanden. Principerna för e-posttjänst, skilda funktioner och de protokoll som används mellan funktionerna finns 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.



Figur 1: Principen för en e-posttjänst

Med utgående e-posttrafik avses i denna föreskrift e-postmeddelanden som sänds av e-posttjänsteleverantörens kunder, och förmedlas via tjänsteleverantörens e-postserverar för utgående trafik (MSA, Message Submission Agent) till e-postsystemets proxyservrar (MTA, Message Transfer Agent).

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

Med ett e-postsystems funktionalitet avses den servicenivå med vilken seriösa e-postmeddelanden sänds, förmedlas och mottas utan avsevärd fördröjning eller avbrott i användningen och seriösa e-postmeddelanden levereras till mottagarna.

Med e-posttjänstens tillgänglighet avses hur e-posttjänstens användare upplever tjänstekvaliteten och hur tjänsten fungerar. Exempelvis störningar i tjänsten och mängden skadliga e-postmeddelanden kan påverka tjänstens tillgänglighet.

3.2.2 Tjänst för förmedling av e-post

Med tjänst för förmedling av e-post avses i denna föreskrift en tjänst som leverantören av e-posttjänster tillhandahåller genom att förmedla eller omdirigera meddelanden via sina egna e-postservrar.

3.2.3 Sekundär tjänst för förmedling av e-post

Med sekundär proxyserver för e-postmeddelanden avses i denna föreskrift en server för förmedling av e-post som säkerställer kundens egen e-posttjänst. I tjänsten har kundens e-postserver eller -servrar definierats som primär mx-post eller primära mx-poster. Då förmedlas inkommande e-posttrafik till kunden via e-posttjänsteleverantörens sekundära proxyserverar endast i de fall då kundens egna servrar inte är tillgängliga.

3.2.4 Öppen proxyserver för e-post

Med öppen proxyserver avses i denna föreskrift ett sådant meddelandeförmedlingssystem 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.

3.2.5 Skadlig e-posttrafik

Med skadlig e-posttrafik avses i denna föreskrift sådan e-posttrafik som kan äventyra kommunikationsnätets eller -tjänstens informationssäkerhet. Med tjänstens informationssäkerhet avses administrativa och tekniska åtgärder för att säkerställa att uppgifterna är tillgängliga endast för dem som har rätt att använda dem (Funktionalitet), att uppgifterna endast kan ändras av dem som har rätt därtill (Konfidentialitet) och att uppgifterna och informationssystemen kan utnyttjas av dem som har rätt att använda dem (Tillgänglighet). I denna föreskrift definieras också sådan e-posttrafik som kan äventyra informationssäkerheten i mottagarens terminalutrustning som skadlig e-posttrafik. Dylig trafik måste absolut anses skadlig, emedan de informationssäkerhetshot som riktas mot de olika parternas terminalutrustning indirekt också äventyrar informationssäkerheten i teleföretagets kommunikationstjänst.

Skadlighet i e-posttrafik ska granskas både ur e-posttjänsteleverantörens och kundens synvinkel. Det innebär i praktiken att tillgängligheten av en kommunikationstjänst kan förutsätta åtgärder såväl för att se till att den tjänst e-posttjänsteleverantören tillhandahåller kan förmedlas som att nivån på den service som förmedlas till användaren upprätthålls. I teorin kunde majoriteten av de informationssäkerhetshot som riktas mot e-posttjänster lösas genom att öka kapaciteten för förmedling av e-posttjänster. Dyliga åtgärder påverkar dock eventuellt inte direkt e-posttjänstens tillgänglighet från användarens synpunkt sett, eftersom användningen av tjänsten i praktiken kan förhindras helt, exempelvis på grund av stora mängder skräppost.

Då man bedömer om e-posttrafik kan anses som skadlig är det väsentliga i praktiken huruvida e-postmeddelandet kan definieras som skadligt med allmänt använda identifierings- och filtreringsmekanismer för skadlig e-post.

3.2.6 Filtrering

Med filtrering avses i denna föreskrift förhindrande av förmedling eller mottagning av e-postmeddelanden, eliminering av sådana skadliga program från meddelanden som äventyrar informationssäkerheten eller andra med dessa jämförbara åtgärder av teknisk karaktär.

3.3 3 § Öppna proxyservrar för e-post

Öppna proxyservrar för e-post används allmänt för förmedling av skadlig e-posttrafik. Genom att identifiera e-postservrar som fungerar som proxyservrar och hindra tredje part från att använda e-postservrarna för förmedling av e-postmeddelanden kan mängden skadlig e-posttrafik minska.

En leverantör av e-posttjänster ska se till att de e-postsystem som leverantören administrerar inte fungerar som öppna proxyservrar. Teståtgärder då system och tjänster tas i bruk och modifieras samt omsorgsfull definiering av inställningarna är exempel på hur man sköter om att e-postsystemen är trygga att använda.

En leverantör av e-posttjänster ska regelbundet testa alla de e-postsystem som leverantören administrerar för att försäkra sig om att systemen inte fungerar som öppna proxyservrar. Om ett företag inte har skaffat något system för testning kan de offentliga tjänster som är tillgängliga på Internet användas.

För Internetförbindelseleverantörens e-postserver för utgående trafik, som hör till Internetanslutningen, avses med denna förpliktelse att det endast är möjligt att sända e-post utan identifierare från ifrågavarande ISP-nät.

3.4 4 § Hantering av inkommande e-posttrafik

Med hantering av inkommande e-posttrafik avses i denna föreskrift åtgärder som kan vidtas för e-postmeddelanden till kunder via tjänsteleverantörens e-postservrar för inkommande trafik (MDA) eller proxyservrar. Åtgärderna är: att identifiera den skadliga källan till e-posttrafik och skadlig e-posttrafik, att filtrera och markera sådan trafik som har identifierats som skadlig samt att leverera trafik till kunderna.

3.4.1 Identifiering av skadlig e-posttrafik

En stor del av såväl de kända berättigade källorna till e-postmeddelanden som de kända skadliga e-postkällorna kan identifieras på basis av källorna till e-posttrafik. Om berättigade källor identifieras kan filtrering av behörig e-posttrafik på grund av felaktig identifiering undvikas. Genom att identifiera källorna till skadlig e-posttrafik kan man förhindra att meddelanden från dessa källor levereras vidare till e-postlådan eller anteckna att det är något betänkligt med e-postmeddelandet, innan det sänds till kundens e-postlåda.

Identifiering av e-postkällor kan basera sig på att berättigade avsändare, icke berättigade avsändare eller vardera, identifieras. Identifieringen kan göras på basis av t.ex. avsändarens webbadress, domännamn eller e-postserver. Skadligheten fastställs utgående från uppgifter som i förväg fått eller samlats in om de meddelanden som förmedlats via källan, eller från analys av innehållet i meddelandet.

Motiveringar

En betydande del av e-posttrafiken mottas från kända webbadresser eller e-postservrar. På basis av erfarenhet, uppföljning eller samlad extern statistik kan en del av dessa identifieras som källor till skadlig e-posttrafik redan i samband med SMTP-kontakten. Likaså mottas en stor del av den seriösa e-posttrafiken från gång på gång använda, behöriga och på förhand kända e-postkällor, som kan identifieras redan då kontakten etableras. Om källorna till skadlig e-posttrafik identifieras redan då kontakt tas behöver en leverantör av e-posttjänster inte ens ta emot ifrågavarande trafik. Detta minskar belastningen på e-posttjänsten och underlättar att seriösa e-postmeddelanden kommer igenom till kunderna.

Identifiering av skadlig e-posttrafik är en förutsättning för alla åtgärder för filtrering och markering som en e-posttjänsteleverantör vidtar. Leverantören av e-posttjänster kan dock upptäcka endast en del av den skadliga e-posttrafiken på basis av e-postkällorna. Därför ska tjänsteleverantören också ha andra metoder för att upptäcka skadlig e-posttrafik.

Många av de här metoderna kan medföra betydande kostnader för e-posttjänsteleverantören. Snäva kriterier för identifiering kan också leda till felaktig bedömning. Genom att använda en

grundläggande metod för identifiering kan e-posttjänsteleverantören minska effekterna av skadlig e-posttrafik och förbättra tjänstens informationssäkerhet och funktion samt den servicenivå och tillgänglighet användarna upplever. På ovan nämnda grunder har e-posttjänsteleverantörerna getts möjlighet att välja den identifieringsmekanism som bäst lämpar sig för den tjänst leverantören erbjuder.

Tillämpning

En leverantör av e-posttjänster ska ha till sitt förfogande aktuella och tillförlitliga mekanismer för att identifiera källorna till e-posttrafik och fastställa e-posttrafikens skadlighet. En e-posttjänsteleverantör kan bland flera alternativ välja de mekanismer som används i systemet så, att en **betydande** del av den skadliga inkommande e-posttrafiken blir identifierad och så lite som möjligt äventyrar seriösa meddelandens möjlighet att gå fram. Förutom de grundläggande identifieringsmekanismerna som är tillgängliga för alla kunder och som uppfyller ovan nämnda kriterier, kan e-posttjänsteleverantören, t.ex. med separat avtal, erbjuda sina kunder också mera avancerade och skräddarsydda mekanismer för identifiering och hantering av skadlig trafik.

Då filtreringsmekanismer för e-posttrafik används vid SMTP-kontakt ska leverantören av e-posttjänster också ha till sitt förfogande en fungerande mekanism för identifiering av de viktigaste kända och seriösa e-postkällorna. Då föreskriften publiceras avses med detta användning av accesslistor.

Det finns flera alternativa metoder för att identifiera e-postkällor och fastställa skadlighet. Det är möjligt att identifiera en betydande del av den skadliga e-posttrafiken redan med att använda en metod. Om man vid identifiering av skadlig trafik samtidigt använder flera metoder som kompletterar varandra förbättras resultaten emellertid ofta. Varje metod har sin egen fördel jämfört med andra metoder, men tyvärr medför alla metoder också problem. E-posttjänsteleverantören ska vara medveten om för- och nackdelarna med de metoder leverantören använder och bedöma effekterna av dessa innan metoderna tas i bruk.

Spärrlistning

Kontakter och e-postmeddelanden från kända, obehöriga e-postkällor kan identifieras och filtreras med hjälp av spärrlistor (blacklist). Med en spärrlista avses normalt en databas med kända skadliga källor till e-posttrafik, som ofta består av webbadresser. Listan kan också bestå av enskilda e-postadresser, domännamn eller e-postservrar som har 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 tredje part upprätthåller. Då man använder och väljer spärrlistor bör man vara extra noggrann för att undvika felaktiga tolkningar. De statiska spärrlistorna är ofta opålitliga, emedan källorna till skadlig e-posttrafik ofta ändras och en eventuell statisk felaktig information på spärrlistan hindrar seriös e-posttrafik för en lång tid. Då information avlägsnas från en statisk spärrlista görs det för hand. Spärrlistor som upprätthålls dynamiskt uppdateras däremot snabbt och felaktiga uppgifter raderas regelbundet från listorna.

Eftersom informationen på en spärrlista kontinuerligt ändras är det i allmänhet inte värt att göra upp någon egen lista. Då spärrlistor används är det skäl att undvika sådana spärrlistor som enskilda användare har gjort upp över vissa stora nätområden. Så säkerställer man e-posttjänstens tillgänglighet. 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 fästa speciell uppmärksamhet vid följande egenskaper hos listan:

- Publicering av principerna för listning
- Det är lätt att avlägsna från listan, och anvisningar finns
- Kontaktuppgifterna till upprätthållaren av listan är offentliga
- Listan baserar sig inte på ett enskilt felaktigt meddelande
- Listan uppdateras regelbundet

Då man använder spärrlistor bör man observera att listorna kan innehålla felaktig information och sålunda hindra seriös e-posttrafik. En lista som upprätthålls av tredje part ska följas med kontinuerligt. De skilda listorna innehåller i allmänhet olika källor, och därför ger användningen av flera listor samtidigt ofta det bästa resultatet. De olika listorna identifierar olika källor och sålunda ökar mängden (procenten) skadlig trafik som kommer till e-postservern från olika källor. Vid heuristisk filtrering kan spärrlistorna också användas som en del av bedömningen av e-postkällans skadlighet. En enskild felaktig listning har då inte som följd att ett seriöst meddelande filtreras.

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

Accesslistning

På accesslistan (whitelist) antecknas att mottagandet av meddelanden är tillåtet via vissa webbadresser, s-postservrar eller e-postadresser, som är allmänt kända som pålitliga avsändare av seriösa meddelanden. Dessa kan exempelvis vara kända e-posttjänsteleverantörer och samarbetspartner.

Användningen av accesslista är i praktiken nödvändig då andra spärr- eller filtreringsmetoder används. Med hjälp av accesslistan kan man försäkra sig om att meddelandena går igenom via pålitliga källor, om meddelandena annars skulle filtreras t.ex. som följd av felaktig spärrlistning.

Då man använder en accesslista bör man hålla i minnet att skadlig e-posttrafik också kan förmedlas via pålitliga aktörer, och man kan således inte heller förbehållslöst lita på källorna på accesslistan. Dessutom kan t.ex. accesslistade adresser förfalskas i skadliga e-postmeddelanden för att göra det lättare för skadlig e-posttrafik att gå igenom. För att undvika problem bör man också följa med innehållet i de meddelanden som accesslistans källor sänder.

Accesslistan är ofta en mycket statisk lista över webbadresser. Det är tjänsteleverantörens uppgift att se till att uppgifterna på listan är uppdaterade, så att de problem som föråldrade uppgifter medför kan undvikas. Kommunikationsverkets CERT-FI-enhet upprätthåller en centraliserad accesslista över finländska aktörers e-postservrar. E-posttjänsteleverantörerna sänder ändrad serverinformation till CERT-FI, som regelbundet distribuerar den uppdaterade listan till användarna. Ett företag som önskar tillgång till CERT-FI:s accesslista eller som önskar bli upptaget på lisan ska kontakta CERT-FI-enheten. Ett annat alternativ till en accesslista som upprätthålls centraliserat är t.ex. DNS Whitelist (<http://www.dnswl.org/>).

Grålistning

Grålistning (greylisting) baserar sig på verksamheten i programvara som sänder skadlig e-posttrafik. I motsats till ett vanligt e-postsystem försöker denna programvara inte sända meddelandet på nytt, även om leveransen av meddelandet hade misslyckats. Vid grålistning statistikförs vissa parametrar automatiskt (IP-adressen/adressens C-klass till avsändaren av inkommande e-post, SMTP-avsändare och SMTP-mottagare) eller en hash-tavla som dessa ingår i. Ett meddelande från en okänd avsändare/med vissa parametrar, tas inte emot. Då källan efter en stund sänder meddelandet på nytt, tas det emot. I fortsättningen tas meddelanden från ifrågakvarande källa emot utan fördröjning.

Problemet med grålistning är att seriösa e-postmeddelanden från på förhand okända källor blir fördröjda. Dessutom baserar sig verksamheten med 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 omsändningen av e-postmeddelanden e-posttrafiken och belastar både nät och e-postservrar.

Omdömessystem

Omdömessystemen baserar sig på meddelandekällans tidigare sändningshistoria. De meddelanden som e-postkällorna (t.ex. avsändarens IP-adress och SMTP-avsändaren) sänder följs med,

statistikförs och jämförs med källans tidigare historia. Vid statistikföring och jämförelse fäster man uppmärksamhet vid om källan sänder seriösa e-postmeddelanden eller skadliga e-postmeddelanden. E-postkällorna kan också övervakas på basis av mängden utgående meddelanden från servern. Uppgifterna används för att genom antalet poäng bedöma e-postkällans omdömesnivå utifrån avsändarens tidigare sändnings- och meddelandehistoria. 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 meddelandena inte filtreras på grund av enstaka osakliga meddelanden. Omdömessystemen stöder andra filtreringssystem väl och minskar som en del av heuristisk filtrering andra kriteriers fel. Då omdömessystemet används bör man dock beakta att systemets bedömning inte nödvändigtvis hinner reagera på den stora mängden skadlig trafik.

De omdömessystem som upprätthålls av tredje part samlar den information de behöver för bedömningen från sina egna kunder. Uppgifterna från flera källor samlas i en gemensam databas för bedömning av omdömesnivån. Ett exempel på en implementering av omdömessystem som upprätthålls av tredje part är TrustedSource (<http://www.trustedsource.org/>) och ett exempel på ett omdömessystem som stöder enskilt identifieringssystem är SpammAssassin AWL (<http://wiki.apache.org/spamassassin/AutoWhitelist>).

Heuristisk analys

En e-posttjänsteleverantör kan också fastställa skadligheten i meddelanden och filtrera dem genom en analys på basis av innehållet i ett e-postmeddelande, 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 från 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 ut 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 seriösa e-postmeddelanden. Filtreringsmetoder som baserar sig på spärrlistor kan också kombineras med exempelvis innehållsmässig filtrering. Då flera mekanismer kombineras antingen höjer eller sänker var och en metod den skadliga nivån i meddelandet. Utgående från den slutliga bedömningen av meddelandet, dvs. antalet poäng meddelandet får, beslutar man om meddelandet är skadligt eller inte. På basis av analysen antingen spärrar filtreringsprogrammet meddelandet, märker ut det som troligen skadligt eller förmedlar meddelandet som sådant.

Övriga mekanismer

Förutom de mekanismer som nämnts ovan kan en e-posttjänsteleverantör välja flera andra metoder för identifiering av e-postkällor, och nya möjligheter kommer ständigt. Nya metoder är bl.a. Sender Policy Framework (SPF) [13] och Domain Keys Identified Mail (DKIM) [14], som identifierar att ett e-postmeddelande har sänts från den e-postserver som e-postadressen indikerar. Såsom andra kontrollmetoder för skadlig e-posttrafik har också de här mekanismerna en hel del svagheter, som bör beaktas då metoderna tas i bruk. Saken beskrivs i RFC 4686 [15]. Eftersom t.ex. förmedling av e-post, elektroniska postkort och en Internetförbindelseleverantörs sändningstjänster förstör dessa mekanismers funktion, lämpar sig mekanismerna bäst för enbart positiv identifiering av källan.

Innan de nya mekanismerna tas i bruk ska en e-posttjänsteleverantör noggrant bekanta sig med metodens verksamhetsprinciper och risker för att undvika filtrering av felaktiga seriösa e-postmeddelanden. Enstaka mekanismers noggrannhet är ofta osäker, om man okritiskt litar på mekanismens tolkning "behörig/obehörig". Om flera mekanismer däremot används samtidigt som en del av bedömningssystemet kan mycket exakta filtreringsresultat med liten felmarginal erhållas.

Rekommendationer

Det rekommenderas att e-posttjänsteleverantörer gör en kontroll för att identifiera skadlig e-posttrafik redan vid SMTP-kontakten. Det blir då 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-postserverna.

Vid identifiering av skadlig e-posttrafik rekommenderas det att flera metoder används samtidigt. Precisionen för identifiering 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. Rekommendationen är att e-posttjänsteleverantörerna tar i bruk t.ex. den accesslista som Kommunikationsverkets CERT-FI-enhet upprätthåller, eller någon motsvarande accesslista.

3.4.2 Filtrering och märkning av e-posttrafik

Med filtrering av inkommande e-posttrafik avses att identifierad skadlig e-posttrafik avsedd för kunderna hindras från att komma till kundernas e-postlåda. Genom att filtrera skadliga e-postmeddelanden är det möjligt att minska belastningen på e-postserverna och mängden skadliga e-postmeddelanden i kundernas e-postlådor och sålunda underlätta kontrollen av vilka meddelanden som är seriösa. Samtidigt förhindras de skadliga e-postmeddelandenas effekt exempelvis då kunderna öppnar bilagor till e-postmeddelanden eller då kunderna via en länk i meddelandet styrs till www-sidor som innehåller skadliga program. Med filtrering av e-posttrafik kan man förbättra servicenivån och informationssäkerheten i tjänsten för kunderna.

Motiveringar

En betydande del av inkommande e-posttrafik kan nuförtiden uppfattas som skadlig e-posttrafik. Skadliga e-postmeddelanden som identifieras och filtreras i ett så tidigt skede som möjligt minskar e-postsystemets belastning och underlättar att seriösa meddelanden går fram. Genom att hindra skadlig e-posttrafik att nå e-postserver är det också möjligt att förebygga skadlig inverkan som riktas mot systemet, exempelvis vid blockeringsattacker. Filtrering av skadliga e-postmeddelanden ökar tjänstens informationssäkerhet och funktion.

Filtrering av skadliga e-postmeddelanden förhindrar att innehåll som är skadligt för kundens informationssäkerhet och för kommunikationsnäten kommer till kundens e-postlåda, samt hanteras. Dessutom minskar mängden e-postmeddelanden i kundens e-postlåda då skadlig e-posttrafik filtreras. Kundens hantering av e-postmeddelandena förenklas då seriösa och skadliga meddelanden inte behöver skiljas åt. Kunderna upplever samtidigt att servicenivån och tillgängligheten förbättras.

Identifiering av e-posttrafik kan basera sig på skadliga e-postkällors identifieringsmekanismer och/eller heuristiska filtreringssystem. Eftersom en del användare av e-posttjänster själva vill försäkra sig om att ingen inkorrekt filtrering görs, har e-posttjänsteleverantörerna fått möjlighet att märka ut sådan trafik som upptäckts vara skadlig i stället för att filtrera den. På kundens begäran eller enligt separat avtal kan e-posttjänsteleverantören också underlåta att märka ut skadlig trafik.

Tillämpning

En e-posttjänsteleverantör ska 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 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 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.

Möjligheten för e-posttjänsteleverantören att skilt komma överens om att trafik som identifierats som skadlig inte filtreras eller märks ut som skadlig innebär ett separat avtal som görs på kundens begäran. E-posttjänsteleverantören kan alltså inte inkludera detta alternativ i sitt standardavtal.

Trots alla ovan nämnda undantag ska e-posttjänsteleverantören ändå alltid filtrera sådan e-posttrafik som identifierats som skadlig som äventyrar funktionsdugligheten i de system som används för att producera e-posttjänsten.

3.4.3 Information om filtreringsprinciper för inkommande e-posttrafik

Identifiering och filtrering eller utmärkning av skadlig e-posttrafik är nödvändig för att säkerställa e-posttjänstens funktion och tillgänglighet. Missförstånd och onödiga kundreklamationer kan undvikas genom att kunderna informeras om grundprinciperna för filtrering av e-posttrafik.

Motiveringar

Kunden har rätt att erhålla information om egenskaperna i den tjänst han eller hon erbjuds och sålunda också om de filtreringsprinciper en e-posttjänsteleverantör använder. Ytterligare föranleder den filtrering av inkommande e-posttrafik som e-posttjänsteleverantören gör frågor från kundernas sida om seriösa e-postmeddelanden filtreras felaktigt eller om mängden skadlig inkommande e-posttrafik till kundens e-postlåda ökar markant.

Tillämpning

En e-posttjänsteleverantör som filtrerar sina kunders e-posttrafik ska för kunden beskriva de allmänna filtreringsprinciperna som används. 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 till kunden får inte äventyra kommunikationstjänstens informationssäkerhet, dvs. beskrivningen behöver inte vara onödigt detaljerad med exakta uppgifter t.ex. om 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, ty de listor som används kan variera från fall till fall.

3.5 5 § Hantering av utgående e-posttrafik

Med hantering av utgående e-posttrafik avses i denna föreskrift åtgärder som kan vidtas för e-postmeddelanden som förmedlas via e-postservrar för utgående trafik (MSA). Dessa åtgärder är identifiering av behöriga avsändare samt filtrering av sådan utgående e-posttrafik via MSA som har identifierats som skadlig.

Motiveringar

Syftet med hantering av utgående e-posttrafik är att minska mängden utgående skadlig e-posttrafik och skräppost via en e-posttjänsteleverantörs server, förbättra e-posttjänsteleverantörernas e-postservrars rykte samt underlätta att seriösa e-postmeddelanden från tjänsteleverantörens kunder går fram. Den servicekvalitet som användarna upplever främjas också.

Effekten av skadlig e-posttrafik kan minskas betydligt, om skadliga e-postmeddelanden identifieras och förmedlingen av dem spärras i ett så tidigt skede som möjligt. Därför ska tjänsteleverantören begränsa rätten att sända e-post endast till aktörer som är berättigade därtill samt filtrera e-posttrafik som har identifierats som skadlig, innan skadliga e-postmeddelanden belastar datakommunikationsnät och motsvarande e-postservrar.

Med dessa åtgärder kan en tjänsteleverantör minska mängden utgående skadliga e-postmeddelanden via sin egen server och sålunda förbättra sitt eget rykte ur deras synpunkt som mottar meddelandena, samt underlätta att seriösa meddelanden från dem som är berättigade till e-posttjänsteleverantörens tjänster förmedlas och går fram.

Om skadlig trafik identifieras och källan till trafiken spåras kan en tjänsteleverantörs kund också informeras om det skadliga programmet i kundens dator. Dessutom kan kunden informeras om

hur skadeprogrammet kan avlägsnas och sålunda förhindra att skadliga meddelanden i fortsättningen sänds från hans eller hennes dator.

Tillämpning

En leverantör av e-posttjänster ska ha till sitt förfogande aktuella och tillförlitliga mekanismer för att identifiera och filtrera skadlig utgående e-posttrafik. Identifiering av skadlig e-posttrafik kan exempelvis basera sig på identifiering av obehörig källa, virusfiltrering av utgående trafik, exceptionellt stor mängd utgående e-posttrafik från användarens dator, eller granskning av att innehållet i rubriken motsvarar Internetstandarder.

En e-posttjänsteleverantör kan bland flera alternativ välja de mekanismer som används i systemet så, att en **betydande** del av den skadliga utgående e-posttrafiken blir identifierad och filtrerad så att förutsättningen att seriösa meddelanden går igenom äventyras så lite som möjligt.

Om en e-posttjänsteleverantör märker att en behörig användares 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, samt i mån av möjlighet kontakta kunden.

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 rensa den infekterade datorn och avhjälpa situationen.

Kundmeddelande

En leverantör av e-posttjänster ska för kunderna beskriva de allmänna principerna för filtrering av utgående e-posttrafik. De principer som beskrivs under punkt 3.4.3 tillämpas vid information om filtreringsprinciperna.

3.6 6 § Förbindelse mellan kund och e-postserver

Med förbindelse mellan kund och e-postserver avses i denna föreskrift 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.

Motiveringar

Användarnamn och lösenord förmedlas mellan kunden och e-postservern. Om förbindelserna mellan kunden och servern är skyddade 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 erbjuder man dessutom kunderna ett tryggt sätt att använda e-posttjänsten oberoende av accessnät och ökar kundernas förtroende för tjänsten.

Det är, emellertid, skäl att informera kunderna om att en skyddad förbindelse mellan kunden och servern inte alltid utgör en säkerhet för att förbindelsen hålls konfidentiell från kommunikationens ena ända 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.

Tillämpning

En leverantör 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 en teleoperatör ska erbjuda alla sina e-postkunder tillgång till skyddade förbindelser. I de instruktioner 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 [16]-protokoll används för att identifiera behöriga användare och öppna en skyddad kundförbindelse från kunden till en proxyserver för e-post.

IMAP eller POP förbindelser (IMAPS/POPS [17], [18]) skyddade av SSL/TLS-protokoll kan t.ex. användas för detta ändamål mellan kunden och e-postlådeservern.

De webbläsarbaserade e-posttjänsternas kundförbindelser ska alltid vara skyddade. Då detta dokument skrivs rekommenderas skyddsmetoden HTTPS-protokoll [19].

3.7 7 § Uppföljning av e-posttjänsternas funktionsduglighet och kvalitet

Motiveringar

E-posttjänsten har utvecklats till en viktig form av kommunikation för hela samhället, och dess funktion måste absolut tryggas. Det är nödvändigt att kontinuerligt följa med tjänstens funktion och kvalitet så att problem upptäcks och åtgärder kan vidtas i ett tidigt stadium.

Ett teleföretag ska kontinuerligt följa upp kvaliteten på och servicesäkerheten vid produktion av allmänna e-posttjänster och förmedling av elektronisk post. Metoderna för uppföljning av tjänsternas funktion och kvalitet är i första hand avsedda för att stöda upprätthåll och utveckling av tjänsterna samt att trygga deras funktion.

Tillämpning

En leverantör av e-posttjänster ska kontinuerligt följa upp kvaliteten på och servicesäkerheten i de allmänna funktioner som gäller e-posttjänster. Kontrollen innebär att tjänstens funktion och kvalitet följs upp samt statistikförs under en lång tid.

Kontinuerlig uppföljning av verksamhetens kvalitet och servicesäkerhet

En leverantör av e-posttjänster ska ha ändamålsenliga och tillräckliga mekanismer för att upptäcka sådana väsentliga problem som påverkar tjänstens funktion och reagera på dem. Med dylika problem avses situationer där e-posttjänstens tillgänglighet eller informationssäkerhet äventyras t.ex. på grund av exceptionell mängd e-posttrafik eller fel i programvara/utrustning.

Leverantörer av e-posttjänster med över 10 000 kunder ska ha tillgång till mekanismerna dygnet runt. Man ska dock alltid beakta problemets allvar och reagera utan onödigt dröjsmål. Med att reagera på problemsituationer avses i denna föreskrift t.ex. ibruktagande av uppräknade filteringsåtgärder, användning av automatiska kontrollmekanismer i system som producerar e-posttjänster och omdirigering av e-posttrafik vid belastningssituationer eller störningar i tjänsten.

Permanent mätare som lämpar sig för att upptäcka problem som beskrivs ovan är bl.a. vilken fördröjningen blir för e-post att komma fram, samt belastning av och köbildning i e-posttjänsten.

Fördröjning för e-postmeddelande

Med uppföljning av fördröjning av leverans av e-postmeddelande i en e-posttjänsteleverantörs eget system avses att mäta den tid det tar för ett e-postmeddelande att nå fram i e-posttjänsteleverantörens eget system. Vid utgående e-posttrafik kan fördröjningen i tid mätas från det ögonblick då meddelandet tas emot för förmedling från kundanslutning eller e-posttillämpning, såsom webmail, till det ögonblick man försöker leverera meddelandet vidare. I sådana fall då den mottagande e-postserverna t.ex. tillfälligt är överbelastad, och uppmanar servern att sända meddelandet på nytt senare, kan meddelandet inte vidarebefordras.

Vid inkommande e-posttrafik kan fördröjningen av den tid det tar för ett meddelande att nå fram mätas från det ögonblick då ett externt e-postsystem öppnar förbindelsen för att förmedla

meddelandet till teleföretagets e-postsystem till det ögonblick då meddelandet är levererat till mottagarens e-postlåda i teleföretagets eget system eller man försöker förmedla meddelandet till en mottagare i teleföretagets externa system. I teleföretagets egna system kan ett meddelande passera flera servrar, t.ex. via en e-postserver för trafik från ett externt system till en e-postlådeserver. Fördröjning av leverans kan uppföljas som en fördröjning för hela systemet eller som en intern fördröjning för en enskild serverkomponent.

Belastning av och köbildning i e-posttjänsten

Med uppföljning av belastning och köbildning avses kontroll av belastningen av serversystem och köer i e-posttrafiken. Med uppföljning av belastning avses t.ex. kontroll av resurser på operativsystemnivå i system som används för att producera e-posttjänster. Med uppföljning av köbildning avses t.ex. automatisk kontroll av e-postköerna i system som används för produktion av e-posttjänster, för att snabbt kunna upptäcka fel och reagera på situationen.

Statistik

För utveckling av e-posttjänsten, säkerställande av tjänstens funktions säkerhet och för myndigheterna ska en e-posttjänsteleverantör följa upp och föra statistik över åtminstone följande parametrar:

- mängd e-posttrafik som identifierats, markerats och filtrerats som skadlig trafik
- mängd sänd och mottagen e-posttrafik
- belastning i e-posttjänsten
- kundmängd

Uppföljning av filtreringsmekanismernas funktion

Med uppföljning av funktionen av de filtreringsmekanismer som används avses kontroll av de filter som används för produktion av e-posttjänster, såsom spärrlistor eller mekanismer för filtrering av innehållet, beträffande mekanismernas funktion och mängden filtrerad trafik. På basis av uppföljningen kan ett teleföretag försäkra sig om mekanismens funktion och orsakerna till filtrering av trafik i oklara fall samt följa upp mängden filtrerad trafik under en viss tidsperiod.

Det är möjligt att följa upp filtreringsmekanismernas funktion t.ex. genom att rapportera om meddelanden som spärrats i e-postloggen på basis av spärrlistor, registrera meddelanden i e-postloggen som märkts ut eller spärrats på basis av sitt innehåll samt följa upp statistik som förts utgående från dessa uppgifter. Funktionen kan också testas så att man sänder testmeddelanden som innehåller skadliga komponenter via system som skyddas av filtreringsmekanismer. Mängden filtrerad trafik kan följas upp exempelvis genom att föra statistik över trafik som klassificeras som skadeprogram, i övrigt skadlig eller normal trafik. Beträffande skadliga program kan ett teleföretag t.ex. samla statistik över hur ofta olika typer av skadeprogram totalt förekommer i e-posttrafiken. Utgående från uppföljningen kan teleföretaget vid behov vidta åtgärder och exempelvis införa effektivare filtreringsmetoder.

3.8 8 § Administrering av e-postadresser

Administrering av e-postadresser är en del e-posttjänstens funktion och tillgänglighet. Olika praxis för administrering av e-postadresser, liknande och/eller vilseledande e-postadresser samt e-postadresser som inte längre har använts men som på nytt har tagits i bruk har skapat problemsituationer. Genom att förenhetliga olika tjänsteleverantörers praxis och beskriva administreringen av e-postadresser för kunderna är det möjligt att förebygga dylika problemsituationer. Färdiga handlingsmönster kan å andra sidan försnabba lösningen av problemen.

3.8.1 Beskrivning av administrering av e-postadresser för kunder

Motiveringar

Praxis för administrering av e-postadresser varierar från en tjänsteleverantör till en annan. Problemsituationerna uppfattas också på olika sätt beroende på tjänsteleverantör. Det är möjligt

att undvika missförstånd och påskynda problemlösningen genom att definiera gemensamma praxis för administrering och beskriva dem för kunderna.

Tillämpning

En leverantör av e-posttjänster ska för kunderna definiera och beskriva praxis 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. Dessutom ska e-posttjänsteleverantören för sina kunder beskriva handlingsmönster och begränsningar som gäller liknande och missvisande e-postadresser.

3.8.2 Överlåtelse av e-postadress som blivit ledig

Motiveringar

Meddelanden sänds ofta till en e-postadress efter det att adressen har stängts. Om en adress som blivit ledig genast eller snart efter att den stängts ges till en annan kund, kan den nya kunden börja erhålla e-postmeddelanden avsedda för den tidigare användaren. För att förhindra missbruk av e-postmeddelandenas konfidentialitet och e-postadresserna ska e-postadress som blivit ledig hållas i karantän innan den kan frigöras för användning på nytt.

Tillämpning

En leverantör av e-posttjänster får överlåta en e-postadress, som blir ledig, till en annan kund först då tre månader har gått efter det att e-postadressen blev ledig. Om den tidigare innehavaren av en e-postadress önskar sin gamla e-postadress som blivit ledig tillbaka inom tre månader efter att adressen blev ledig har han eller hon rätt att få e-postadressen tillbaka, ifall kundförhållandet inte har brutits. Rätten att få en e-postadress tillbaka förpliktar emellertid inte i sig tjänsteleverantören att spara e-postmeddelanden på e-postkontot efter det är kontot har avslutats. En sådan skyldighet kan dock t.ex. basera sig på en överenskommelse parterna emellan.

3.8.3 Administrering av problemsituationer med vilseledande e-postadresser

Motiveringar

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 e-postadress som är registrerad i en annan persons eller annat företags namn, företags FO-nummer eller vissa allmänt kända adresser (såsom postmaster, webmaster eller kundtjänst). Handlingsmönster som har gjorts upp på förhand påskyndar och förenklar behandlingen av fallen.

Tillämpning

Om en e-posttjänsteleverantör upptäcker eller informeras om en vilseledande e-postadress som registrerats på hans domännamn ska e-posttjänsteleverantören ingripa. E-posttjänsteleverantören har rätt att ta adresser ur bruk, 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.

Kommunikationsverket rekommenderar, att e-posttjänsteleverantörerna inte beviljar sina kunder sådana vilseledande e-postadresser eller deras finskspråkiga motsvarigheter, som definieras i RFC 2142 [20] och hänför sig till e-posttjänsteleverantörens eget domännamn.

3.9 9 § E-posttjänsteleverantörens kontaktuppgifter

En leverantör av e-posttjänster ska se till att företaget har domännamnspecifika postmaster- och abuse-e-postadresser för sina egna domännamn och för de domännamn som används för tillhandahållande av e-posttjänster. Meddelanden som kommer till dessa adresser kontrolleras regelbundet.

Med detta krav sörjer man för att ett teleföretag har tillgång till en kontaktpunkt för information om eventuella störningar i verksamheten eller användningen, oberoende var meddelaren befinner sig.

Postmaster- och abuse-adresserna har en stor spridning och samlar ofta obefogad kommunikation. Därför bör teleföretaget ombesörjer uppföljningen av adressen så att behandlingen av seriösa 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 part som ansvarar för domännamnet.

3.10 10 § Ikraftträdande och övergångsbestämmelser

Denna föreskrift träder i kraft den 1 november 2008.

Om den skyldighet som ålagts i 6 § i föreskriften (att erbjuda skyddade förbindelser) kräver ändringar i e-posttjänsteleverantörens datasystem och kundmeddelanden beviljas denna skyldighet en övergångsperiod till 1.3.2009.

4 ÖVRIGA REKOMMENDATIONER

I detta kapitel beskrivs övriga icke-förpliktande rekommendationer till e-posttjänsteleverantörer, som inte direkt har samband med någon av paragraferna i denna föreskrift.

4.1.1 Skydd av förbindelser mellan servrar

Skydd av förbindelserna mellan servrar för sändning, förmedling och mottagning av e-post främjar e-posttjänsten informationssäkerhet och tillförlitlighet. Då förbindelsen mellan servrarna är skyddad identifierar servrarna varandra då kontakten tas. Identifieringen innebär att den andra parten i kommunikationen är pålitlig. Genom att skydda förbindelserna mellan servrarna kan man också förhindra att e-postmeddelandena kommer tredje parts kännedom.

E-posttjänsteleverantörerna och användarna ska dock beakta, att alla kontakter mellan servrarna inte är skyddade.

Rekommendation

Om en e-postserver (MSA, MTA eller MDA) stöder användning av skyddad förbindelse rekommenderas det att egenskapen i mån av möjlighet tas i bruk, för att trygga konfidentiell e-posttrafik.

5 REFERENSLISTA

[1] Kommunikationsmarknadslagen (393/2003 jämte ändringar), uppdaterad version: <http://www.finlex.fi/sv/laki/ajantasa/2003/20030393>.

[2] Lagen om dataskydd vid elektronisk kommunikation (516/2004 jämte ändringar), uppdaterad version: <http://www.finlex.fi/sv/laki/ajantasa/2004/20040516>.

[3] Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0021:SV:NOT>

[4] Europaparlamentets och rådets direktiv 2002/20/EG av den 7 mars 2002 om auktorisation för elektroniska kommunikationsnät och kommunikationstjänster (auktorisationsdirektiv) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0020:SV:NOT>

[5] Europaparlamentets och rådets direktiv 2002/19/EG av den 7 mars 2002 om tillträde till och samtrafik mellan elektroniska kommunikationsnät och tillhörande faciliteter (tillträdesdirektiv) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0019:SV:NOT>

[6] Europaparlamentets och rådets direktiv 2002/22/EG av den 7 mars 2002 om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster (direktiv om samhällsomfattande tjänster)
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0022:SV:NOT>

[7] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation)
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:SV:NOT>

[8] Kommunikationsverkets föreskrift 9 B/2004 M om skyldighet att anmäla kränkningar av informationssäkerhet samt fel och störningar i allmän televerksamhet,
<http://www.ficora.fi/attachments/ruotsi/1156489175448/Files/CurrentFile/Kommunikationsverket09B2004M.pdf>

[9] Kommunikationsverkets föreskrift 13 A/2008 M om Internetförbindelsetjänsternas informationssäkerhet och funktionsduglighet
<http://www.ficora.fi/attachments/ruotsi/5B36zjZG/Files/CurrentFile/Kommunikationsverket13A2008M.pdf>

[10] Kommunikationsverkets föreskrift 47 B/2004 M om informationssäkerhet hos teleföretag
<http://www.ficora.fi/attachments/ruotsi/1156489186667/Files/CurrentFile/Kommunikationsverket47B2004M.pdf>

[11] Kommunikationsverkets föreskrift 53/2008 M om skyldighet att lagra identifieringsuppgifter
<http://www.ficora.fi/attachments/ruotsi/5yk2njGhM/Files/CurrentFile/Kommunikationsverket532008M.pdf>

[12] Kommunikationsverkets föreskrift 54/2008 M om säkerställande av kommunikationsnät och kommunikationstjänster
<http://www.ficora.fi/attachments/ruotsi/5vB4Pcjinx/Files/CurrentFile/Kommunikationsverket542008M.pdf>

[13] RFC 4408, Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1, <http://www.ietf.org/rfc/rfc4408.txt>

[14] RFC 4871, DomainKeys Identified Mail (DKIM) Signatures, <http://www.ietf.org/rfc/rfc4871.txt>

[15] RFC 4686, Analysis of Threats Motivating DomainKeys Identified Mail (DKIM),
<http://www.ietf.org/rfc/rfc3761.txt>

[16] RFC 2554, SMTP Service Extension for Authentication, <http://www.ietf.org/rfc/rfc2554.txt>

[17] RFC 2595, Using TLS with IMAP, POP3 and ACAP, <http://www.ietf.org/rfc/rfc2595.txt>

[18] RFC 4616, The PLAIN Simple Authentication and Security Layer (SASL) Mechanism,
<http://www.ietf.org/rfc/rfc4616.txt>

[19] RFC 2818, HTTP Over TLS, <http://www.ietf.org/rfc/rfc2818.txt>

[20] RFC 2142, Mailbox names for Common Services, Roles and Functions,
<http://www.ietf.org/rfc/rfc2142.txt><http://www.ietf.org/rfc/rfc2595.txt>

6 FÖRKORTNINGAR

CERT-FI	Computer Emergency Response Team - Finland
DNS	Domain Name Server
IMAP	Internet Message Access Protocol
IMAPS	Secure IMAP
IP	Internet Protocol
ISP	Internet Service Provider
MDA	Message Delivery Agent
MSA	Message Submission Agent

MTA	Mail Transfer Agent
MX	mail exchange
POP	Post Office Protocol
POPS	Secure POP
RFC	Request for Comments
SMTP	Simple Mail Transfer Protocol
SMTP-AUTH	SMTP Authentication
SSL	Secure Socker Layer
TLS	Transport Layer Security