

**MOTIVERING TILL OCH TILLÄMPNING AV
FÖRESKRIFT 9**

**OM SKYLDIGHET ATT ANMÄLA
KRÄNKNINGAR AV INFORMATIONSSÄKERHET I ALLMÄN TELEVERKSAMHET**

Innehåll

INNEHÅLL	1
1 LAGSTIFTNING	2
1.1 Rättsgrund	2
1.2 Andra relaterade bestämmelser	2
1.2.1 Övrig lagstiftning.....	2
1.2.2 Kommunikationsverkets tekniska föreskrifter	3
1.2.3 Behandling av givna uppgifter vid Kommunikationsverket.....	4
2 SYFTET MED FÖRESKRIFTEN OCH ÄNDRINGSHISTORIA	5
2.1 Syftet med föreskriften	5
2.2 Centrala ändringar och ändringshistoria	5
3 MOTIVERING TILL ENSKILDA PARAGRAFER OCH ANVISNINGAR FÖR TILLÄMPNING .	6
3.1 1 § Tillämpningsområde	6
3.1.1 Motivering och tillämpning	6
3.2 2 § Anmälan till abonnenter.....	7
3.2.1 Motivering	7
3.2.2 Tillämpning.....	7
3.3 3 § Anmälan till Kommunikationsverket	8
3.3.1 Motivering	8
3.3.2 Tillämpning.....	8
4 ÖVRIGA REKOMMENDATIONER.....	11
4.1 Rekommendation om samarbete vid kränkningar av informationssäkerhet	11
4.2 Rekommendation om att underrätta Kommunikationsverket om situationer som hänför sig till informationssäkerhet.....	11
4.3 Rekommendation om att underrätta om kränkningar mot andra än teleföretag	11
5 REFERENSLISTA	12

1 LAGSTIFTNING

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

1.1 Rättsgrund

Kommunikationsverkets föreskrift baserar sig på 21 § i lagen om dataskydd vid elektronisk kommunikation (516/2004, dataskyddslagen) [1]. Dataskyddslagen som trädde i kraft 1.9.2004 verkställde för sin del EG:s direktiv om dataskydd vid elektronisk kommunikation [2] som godkändes i februari 2002.

Enligt 21 § 1 mom. i dataskyddslagen är ett teleföretag skyldigt att utan dröjsmål informera abonnenterna om ett speciellt hot mot tjänstens informationssäkerhet. Samtidigt ska teleföretaget informera:

- om de åtgärder som abonnenterna och användarna kan tillgripa för att avvärja hotet samt
- om de sannolika kostnaderna för åtgärderna.

Enligt 21 § 2 mom. i dataskyddslagen ska ett teleföretag informera Kommunikationsverket om betydande kränkningar av dataskyddet för nät- och kommunikationstjänster samt om sådana mot dessa tjänster riktade hot som teleföretaget är medvetet om. Samtidigt ska teleföretaget ge information om åtgärder genom vilka det försöker hindra en upprepning av sådana kränkningar och hot. När ett teleföretag har avvärjt en betydande, mot dess tjänster riktad dataskyddskränkning eller ett hot eller när det har avlägsnat en störning ska det på ett ändamålsenligt sätt informera om vilka åtgärder som vidtagits och om eventuella effekter på användningen av tjänsterna.

Enligt 21 § 4 mom. i dataskyddslagen kan Kommunikationsverket ge teleföretag:

- föreskrifter om innehållet i och utformningen av anmälningar till abonnenterna om ett speciellt hot mot tjänsten,
- föreskrifter om innehållet i och utformningen av anmälningar om betydande kränkningar av och hot mot informationssäkerheten samt om hur anmälningarna ska ges in till Kommunikationsverket, samt
- anvisningar om innehållet i och formen för den information som ges efter det att teleföretaget har avvärjt en betydande kränkning av eller ett hot mot informationssäkerheten.

1.2 Andra relaterade bestämmelser

1.2.1 Övrig lagstiftning

Skyldighet att handha dataskyddet, 19 § i dataskyddslagen Enligt i paragrafen ska ett teleföretag handha dataskyddet för sina tjänster. Handhavandet av dataskyddet för tjänster avser åtgärder för att trygga säkerheten av verksamheten, datatrafiken, utrustningen och programmen samt för datamaterialet. Dessa åtgärder ska anpassas till hur allvarliga hot som föreligger samt till den tekniska utvecklingens nivå och till kostnaderna. Skyldighet att handha dataskyddet gäller också behandling av uppgifter som behövs för fullgörandet av lagringsskyldigheten. Ett teleföretag är gentemot abonnenterna och användarna ansvarigt för dataskyddet också i fråga om sådan tredje part som helt eller delvis utför nättjänsten, kommunikationstjänsten, lagringen av uppgifter eller mervärdestjänsten.

Åtgärder för att genomföra dataskyddet, 20 § i dataskyddslagen Enligt paragrafen är ett teleföretag och de som handlar för dess räkning rätt att vidta de nödvändiga åtgärder som avses i lagen med avseende på dataskyddet i följande situationer:

- 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 göra störningarna föremål för förundersökning,
- 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 [3], vilka planeras bli genomförda i omfattande utsträckning via kommunikationstjänsterna.

De nödvändiga åtgärderna kan 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.

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 20 § i dataskyddslagen 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, om det inte är så att underrättelsen sannolikt äventyrar uppnåendet av målen. Teleföretagen ska utföra åtgärderna 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 målen för behandlingen. Åtgärderna ska avbrytas, om det inte längre finns i denna paragraf nämnda förutsättningar för att vidta dem.

Skyldighet att undanröja störning, 131 § i kommunikationsmarknadslagen (393/2003) [4]. 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 enligt paragrafen omedelbart vidta åtgärder för att korrigera situationen och vid behov koppla bort kommunikationsnätet eller utrustningen från det allmänna kommunikationsnätet.

1.2.2 Kommunikationsverkets tekniska föreskrifter

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 13 *om Internetförbindelsetjänsternas informationssäkerhet och funktionsduglighet* [6]. 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 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. Föreskriften tillämpas även på televerksamhet som är av ringa betydelse. 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 teleföretags beredskap för fel och störningar och procedurer vid fel och störningar.

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

1.2.3 Behandling av givna uppgifter vid Kommunikationsverket

Kommunikationsverket behandlar de uppgifter som anmäls enligt 21 § i dataskyddslagen konfidentiellt. Enligt *lagen om offentlighet i myndigheternas verksamhet* (621/1999, offentlighetslagen) [9] är uppgifterna sekretessbelagda.

- Enligt 24 § 1 mom. 7 punkten i *offentlighetslagen* är följande myndighetshandlingar sekretessbelagda, om inte något annat föreskrivs särskilt: handlingar som gäller skyddsarrangemang för personer, byggnader, inrättningar, konstruktioner samt data- och kommunikationssystem och genomförandet av arrangemangen, om det inte är uppenbart att utlämnandet av uppgifter ur en sådan handling inte äventyrar genomförandet av syftet med skyddsarrangemangen.
- Enligt 24 § 1 mom. 20 punkten är också följande handlingar sekretessbelagda: handlingar som innehåller uppgifter om en privat affärs- eller yrkeshemlighet samt sådana handlingar som innehåller uppgifter om någon annan motsvarande omständighet som har samband med privat näringsverksamhet, om utlämnandet av uppgifter ur en sådan handling skulle medföra ekonomisk skada för näringsidkaren, och det inte är fråga om uppgifter som är betydelsefulla för skyddande av konsumenters hälsa eller en hälsosam miljö eller för bevakande av de rättigheter som innehas av dem som orsakas skada av verksamheten eller uppgifter om näringsidkarens skyldigheter och fullgörande av dessa.

Enligt 34 a § i dataskyddslagen har Kommunikationsverket rätt att till de teleföretag, dem som tillhandahåller mervärdestjänster och de sammanslutningsabonnenter som har utnyttjats vid kränkning av dataskydd, som har blivit föremål för sådan kränkning eller som sannolikt kan utsättas för kränkning av dataskydd under vissa förutsättningar lämna ut identifieringsuppgifter som verket har erhållit i samband med insamlandet av uppgifter om och utredning av kränkningar av dataskydd. Kommunikationsverket har också rätt att till sådana myndigheter eller andra instanser som är verksamma i andra stater och som har till uppgift att förebygga eller utreda kränkningar av dataskydd riktade mot kommunikationsnät och kommunikationstjänster lämna ut identifieringsuppgifter som verket erhållit i samband med insamlandet av uppgifter om och utredning av kränkningar av dataskydd.

Kommunikationsverket har dock rätt att lämna ut identifieringsuppgifter endast i den omfattning som behövs för att förebygga och utreda kränkningar av dataskydd. Utlämnandet av uppgifter får inte begränsa skyddet av konfidentiella meddelanden eller integritetsskyddet mer än nödvändigt.

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 föreskriften är att definiera innehållet i och förfaringsätt vid de anmälningar som teleföretagen ska ge in till Kommunikationsverket och till kunderna, om teleföretagets tjänst är utsatt för en betydande kränkning av eller ett hot mot informationssäkerheten så som avses i 21 § i lagen om dataskydd vid elektronisk kommunikation.

2.2 Centrala ändringar och ändringshistoria

Ny gruppering av föreskrifter:

I början av 2010 revideras föreskrifter så att bestämmelser om teleföretagens skyldighet att anmäla fel och störningar tas bort från föreskrift 9 och inkorporeras i en särskild föreskrift 57 om underhåll av kommunikationsnät och -tjänster samt om förfarande vid fel och störningar.

De bestämmelser om skyldigheten att anmäla kränkningar av informationssäkerhet som kvarstår i föreskrift 9 ändras inte avsevärt. Det blir dock egna paragrafer för information till abonnenterna och information till Kommunikationsverket. I motiveringspromemorian har dessutom tillagts en rekommendation om teleföretagens samarbete vid informationssäkerhetskränkningar.

3 MOTIVERING TILL ENSKILDA PARAGRAFER OCH ANVISNINGAR FÖR TILLÄMPNING

I detta kapitel behandlas motiveringen till enskilda paragrafer samt rekommendationer för tillämpningen av dem.

3.1 1 § Tillämpningsområde

3.1.1 Motivering och tillämpning

Allmän televerksamhet:

Denna föreskrift tillämpas på teleföretags allmänna televerksamhet. Med allmän televerksamhet avses tillhandahållande av nättjänster eller kommunikationstjänster för en grupp av användare som inte har avgränsats på förhand. Med en *nättjänst* avses en tjänst där ett nätföretag tillhandahåller ett kommunikationsnät som det äger eller på någon annan grund förfogar över för överföring, distribution eller tillhandahållande av meddelanden. Med en *kommunikationstjänst* avses en tjänst som ett tjänsteföretag tillhandahåller för att överföra meddelanden i ett kommunikationsnät som det förfogar över eller har fått tillgång till av ett nätföretag eller för att distribuera eller tillhandahålla meddelanden i ett masskommunikationsnät.

Ett kommunikationsnät definieras i 2 § i *kommunikationsmarknadslagen* och avser nät som tillhandahålls för både målgruppskommunikation och masskommunikation. Föreskriften kan därför tillämpas exempelvis på fasta och trådlösa telefontnät och datanät, kabeltelevisionnät, och under vissa förutsättningar på markbundna digitala televisionnät och analog radio. Det väsentliga i definitionen av ett allmänt kommunikationsnät är att nätet tillhandahålls en grupp av användare som inte har avgränsats på förhand. Det väsentliga i definitionen av en kommunikationstjänst är att teleföretaget tekniskt deltar i överföringen eller tillhandahållandet av meddelanden i egenskap av tjänsteleverantör.

Föreskriften tillämpas även på televerksamhet som är av ringa betydelse för vilken inte behövs en televerksamhetsanmälan enligt 13 § i *kommunikationsmarknadslagen*. Föreskriften gäller dock inte innehållstjänster eller tjänster som tillhandahålls en grupp av användare som har avgränsats på förhand.

Begränsning av tillämpningen beträffande kommunikationsnät:

Varken dataskyddslagen eller föreskriften tillämpas på meddelanden som förmedlas i ett masskommunikationsnät, om meddelandet inte i det enskilda fallet inte kan sättas i förbindelse med den abonnent eller användare som tar emot meddelandet. Därför tillämpas föreskriften på masskommunikationsnät endast om näten används för annat än television- eller radioverksamhet.

Med ett *masskommunikationsnät* avses i *kommunikationsmarknadslagen* ett kommunikationsnät som i huvudsak används för sändning eller tillhandahållande av television- och radioprogramutbud eller annat material som förmedlas i samma form till alla mottagare. Med ett meddelande avses 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. Definitionen omfattar också sådana meddelanden med innehåll som fritt förmedlas till en mottagarkrets som inte är utvald på förhand. Exempel är television- och radioprogram samt alla sidor som är öppna för allmänheten i de elektroniska kommunikationsnäten.

Myndighetsnät:

Föreskriften tillämpas inte heller på *myndighetsverksamhet* i myndighetsnät som avses i *kommunikationsmarknadslagen* eller i andra kommunikationsnät som konstruerats för att tillgodose behov i anslutning till allmän ordning och säkerhet, landets försvar, räddningsuppgifter, befolkningskydd eller trafiksäkerhet till lands, till sjöss, på räs eller i luften. Med ett myndighetsnät avses i *kommunikationsmarknadslagen* ett kommunikationsnät som byggts för behov i anslutning till allmän ordning och säkerhet, räddningsuppgifter eller befolkningskyddet

och i vilket anslutningar kan tillhandahållas utom myndigheterna även andra användargrupper som är nödvändiga med hänsyn till skötseln av ovan avsedda uppgifter. Ett myndighetsnät som överensstämmer med kommunikationsmarknadslagen kan vara ett så kallat rent separat nät eller det kan vara anslutet till ett allmänt kommunikationsnät, vilket betyder att det är till exempel möjligt att ringa från myndighetsnätet till det allmänna telefonnätet.

Föreskriften tillämpas dock på annan allmän televerksamhet än på myndighetsverksamhet i myndighetsnät.

3.2 2 § Anmälan till abonnenter

3.2.1 Motivering

Att säkerställa verksamhetsförutsättningar för abonnenter och användare av teleföretagets tjänster kräver att abonnenterna och användarna har kännedom om informationssäkerhetsrisker som tjänsterna är utsatta för. Lagen om dataskydd vid elektronisk kommunikation avser att *om tjänsten utsätts för ett särskilt hot som de som tillhandahåller tjänsterna inte kan avvärja genom sina egna åtgärder, eller tillsammans med andra operatörer, ska de utan dröjsmål meddela sina abonnenter. Teleföretaget ska samtidigt underrätta abonnenten och användaren om de åtgärder som de kan tillgripa för att avvärja hotet samt om de sannolika kostnaderna för åtgärderna.*

3.2.2 Tillämpning

Bedömning av ett speciellt hot

Speciella informationssäkerhetshot som ska underrättas abonnenterna kan vara:

- vid olika tidpunkter aktuella hot och skydd mot hot som gäller terminalutrustning och programvara med vilka abonnenterna använder internet
 - hot som hänför sig till skadliga program och spridning av dessa till exempel via e-post, internetsidor, mobiltelefoner och peer-to-peer-nät
 - omdirigeringar av uppgift om ringnumret i modembaserad internettrafik
- allvarliga informationssäkerhetsbrister i allmänt tillgängliga system och programvara, till exempel okorrigerade sårbarheter i programvara eller system (informationen publicerad exempelvis av CERT som ett CERT-meddelande eller av systemleverantör)
- aktuella informationssäkerhetshot som hänför sig till användningen av kommunikationstjänster och kräver speciell uppmärksamhet av användarna
 - omfattande aktivering av skadliga program som kräver att kunden vidtar omedelbara åtgärder
 - betydande ökning av mängden skräppost som påverkar tillgängligheten av e-posttjänster
 - övriga händelser i kommunikationsnät som avsevärt äventyrar abonnenternas informationssäkerhet eller dataskydd
- speciella hot som beror på kommunikationstjänsternas internationella karaktär
 - informationssäkerhetshot som beror på att en kommunikationstjänst som är avsedd för finländska användare helt eller delvis utförs utanför Finlands gränser och teleföretaget inte genom sina egna åtgärder kan avvärja hotet.

Information om sårbarheter i programvara rekommenderas i synnerhet om en allmänt använd programvara innehåller en okorrigerad sårbarhet som lätt kan utnyttjas för att orsaka hot mot nätens och tjänsternas informationssäkerhet i allmänhet.

Tidpunkt för anmälan

En del av hoten mot teleföretagets tjänster är sådana vars omedelbara korrigerande inte är möjlig. Offentlig information om sådana hot kunde vara ägnad att äventyra kommunikationens konfidentialitet eller kunde möjliggöra omfattande ekonomiskt missbruk. I sådana fall är det skäl att först försöka fixa säkerhetshållet, varvid man också undviker ytterligare skador för abonnenterna.

När ett teleföretag, enligt dataskyddslagen, har avvärjt en betydande, mot dess tjänster riktad informationssäkerhetskränkning eller ett hot ska det på ett ändamålsenligt sätt informera om vilka åtgärder som vidtagits och om eventuella effekter på användningen av tjänsterna. Informationen ska till sin karaktär vara allmänt och den ska uttryckligen ges i efterhand. Information om åtgärderna ska dock ske i så nära realtid som möjligt. Efterhandsinformationen gör det möjligt för en aktör som blivit utsatt för en kränkning eller ett hot att reagera på situationer som kräver åtgärder i efterhand.

Anmälningförfarande

Kundinformationen kan söktas exempelvis på teleföretagets webbplats, via e-post eller i meddelanden som sänds tillsammans med räkningar. Webbplatser och meddelanden som sänds med räkningen är mycket bra i situationer där hotet varken är kritiskt eller behöver omedelbara åtgärder av abonnenten. Exempel på sådana är meddelanden som gäller allmänna hot vid användningen av internet och åtgärder som abonnenten kan tillgripa för att avvärja dem. Webbplatser lämpar sig också bra för information om mera kritiska hot, t.ex. när trafiken i kommunikationsnäten ökar snabbt på grund av skadliga program. Information via e-post lämpar sig för tillfällen där hotet enbart gäller en begränsad grupp av teleföretagets abonnenter och där information till andra än berörda parter kunde äventyra abonnenternas informationssäkerhet eller dataskydd. I omfattande kritiska fall kan det också vara motiverat att använda massmedier som en informationskanal.

När en kunds internetanslutning öppnas, är det skäl att ge kunden grundläggande anvisningar om hur en man skyddar sin dator mot de vanligaste hoten vid internetanvändningen. Det är skäl att ge sådan information regelbundet, till exempel en gång om året i samband med övrig information till kunden.

Det är skäl att teleföretaget underrättar abonnenterna, om deras anslutningar har kopplats bort från nätet på grund av informationssäkerhetsproblem. Abonnenterna ska få information om såväl teleföretagets åtgärder för att avhjälpa situationen som de åtgärder som teleföretaget förväntar sig att abonnenterna ska tillgripa för att ordna informationssäkerheten för anslutningen.

Rekommendation

Kommunikationsverket rekommenderar dessutom att teleföretaget informerar sina kunder om de vanligaste bluff- och bedrägeriförsöken vid användningen av kommunikationstjänsterna och om det rätta sättet att reagera på dem. Exempel på sådana fall är:

- textmeddelande från okänt nummer med begäran om att ringa ett nummer som ofta är avgiftsbelagt,
- bluffsamtal från avgiftsbelagda eller utländska nummer som syftar till motringning, samt
- aktuella phishingattacker.

3.3 3 § Anmälan till Kommunikationsverket

3.3.1 Motivering

Uppgifter som frågas i en anmälan om kränkning av informationssäkerhet behövs för att skapa en samlad, aktuell och analyserad bild av nuläget i fråga om den riksomfattande informationssäkerheten hos kommunikationsnäten och -tjänsterna. Uppgifterna befrämjar en rätt inriktning och accentuering av på riktig information baserade motåtgärder. Genom anmälan kan organisationen följa sin egen process för informationssäkerhetsshantering och skapa en lägesbild av informationssäkerheten för den egna organisationen. Uppgifter som anmäls är basinformation som behövs för analys av en informationssäkerhetskränkning.

3.3.2 Tillämpning

Enligt dataskyddslagen ska teleföretagen informera Kommunikationsverket om betydande kränkningar av informationssäkerheten för nät- och kommunikationstjänster samt om sådana hot mot dessa tjänster som teleföretagen har kännedom om. *Samtidigt ska teleföretagen informera*

Kommunikationsverket om de åtgärder som de vidtar för att förebygga upprepning av sådana kränkningar och hot.

Bedömning av sakens betydelse

Vid bedömningen av kränkningen, av hot om sådan och av felet eller bristen ska man enligt motiveringen till dataskyddslagen fästa avseende vid skyddet för abonnenternas och användarnas rättigheter, vid tjänstens användbarhet och vid omfattningen av dess geografiska verkningar. Anmälan ska göras omedelbart då sakens betydelse har konstaterats. Av anmälningen ska klart framgå de åtgärder som vidtagits i saken och i mån av möjlighet också hur man i framtiden ska kunna förhindra att problemet återuppstår. Om man inte i samband med anmälningen kan meddela om framtida åtgärder, ska denna kompletteras utan onödigt dröjsmål.

I förteckningen nedan ges exempel på sådana typiska fall som kräver en anmälan. Förteckningen är inte täckande utan syftet är att beskriva allvarlighetsgraden för de fall som ska anmälas. Sådana kränkningar av informationssäkerhet som ska anmälas till Kommunikationsverket är till exempel:

- dataintrång i teleföretagets datasystem
- kränkningar av informationssäkerhet mot teleföretagets datasystem
 - identifierings-, kund- eller specifikationsuppgifter kommer i orätta händer
 - dokumentation om eller konstruktionsbeskrivningar av nätet kommer i orätta händer
 - obehörigt tillträde till systemet som administratör
 - obehörigt tillträde till systemet med användaridentifikation som låter tillgång till kommunikationens innehåll eller identifieringsuppgifter eller som möjliggör obehörig ändring av specifikationer av teleföretagets datasystem eller kommunikationsnät
- kränkningar av informationssäkerhet som har en betydande inverkan på tillgängligheten av kommunikationsnätet eller kommunikationstjänsterna
 - blockeringsattacker
 - snabb ökning av mängden skräppost
 - attacker som påverkar routning av trafiken i kommunikationsnätet
- aktivering av skadliga program (t.ex. datorvirus, bakdörrar, "trojanska hästar", spionprogram eller snifferprogram) i teleföretagets datasystem
- försök att av teleföretagets personal få information som äventyrar teleföretagets eller kundernas informationssäkerhet ("social engineering")
- upptäckt avlyssning eller upptäckta kontrollanläggningar och -kopplingar samt programvara i kommunikationsnätet eller i teleföretagets datasystem eller utrymmen

I förteckningen nedan ges exempel på sådana typiska fall som kräver en anmälan. Förteckningen är inte täckande utan syftet är att beskriva allvarlighetsgraden för de fall som ska anmälas. Sådana informationssäkerhetsshot som ska anmälas till Kommunikationsverket är till exempel:

- upptäckta betydande inbrottsförsök
 - systematiska, från vanlig nätanvändning avvikande försök att med tekniska metoder få uppgifter om exempelvis följande egenskaper hos kommunikationsnät och kommunikationstjänster
 - nätets fysiska och logiska topologi
 - maskinvara och olika versioner av programvara
 - eventuella sårbarheter i system
 - systematiska fientliga inskrivningsförsök i teleföretagets datasystem
 - inbrottsförsök i teleföretagets komponent av viktighetsklass 1 eller 2 i enlighet med Kommunikationsverkets föreskrift 54/2008 M om säkerställande av kommunikationsnät och kommunikationstjänster
- upptäckt nättrafik som avviker från det vanliga
 - avsevärd mängd trafik till oanvända nätadressblock
 - betydande trafikvolym med okända eller sällan använda protokolltyper
 - snabbt ökande trafik till sällsynta nummer eller adresser i utlandet
- avsevärda informationssäkerhetsbrister i teleföretagets datasystem och programvara vilka inte har offentliggjorts exempelvis av CERT som CERT-meddelande eller av systemleverantör

- säkerhetshål genom vilka det är möjligt att obehörigt komma in i systemet som administratör
- säkerhetshål som gör det möjligt att obehörigt få tag i innehållet eller identifieringsuppgifter i kommunikationen eller att obehörigt ändra specifikationer av teleföretagets datasystem eller kommunikationsnät
- omfattande spridning eller aktivering av skadliga program som orsakar ett betydande hot mot teleföretagets tjänster eller kunder i kommunikationsnätet
- speciella hot som beror på kommunikationstjänsternas internationella karaktär
 - upptäckt av ett informationssäkerhetshot som beror på att en kommunikationstjänst som är avsedd för finländska användare helt eller delvis utförs utanför Finlands gränser och teleföretaget inte genom sina egna åtgärder kan avvärja hotet.

Anmälningsförfarande

Om kränkningen eller hotet är allvarligt, eller om meddelandeförmedlingssystemet som används för att göra anmälan misstänks innehålla en kränkning eller om situationen kräver omedelbara åtgärder från Kommunikationsverkets sida, är det skäl att göra den första anmälan omedelbart per telefon med de uppgifter som finns. Den kompletterande skriftliga anmälan kan göras när teleföretaget har en närmare helhetsbild av läget. I långvariga fall ska teleföretaget hålla Kommunikationsverket informerat om hur läget utvecklas. Om en elektroniskt inlämnad anmälan kan ställas i skriftlig och läsbar form, anses den vara en skriftlig anmälan.

Ett rekommenderat sätt för att anmäla kränkningar av och hot mot informationssäkerhet är att använda den blankett som finns i bilaga 1. Anmälan kan också vara ett fritt formulerat e-postmeddelande, om det har samma innehåll som frågas i blanketten.

Ett teleföretag ombeds ge Kommunikationsverket kontaktuppgifterna till dem som behandlar kränkningar av informationssäkerhet samt hålla uppgifterna uppdaterade på den blankett som finns i bilaga 2.

Kontaktinformation

E-POST: CERT@FICORA.FI

Uppgifter om CERT-FI-enhetens PGP-nycklar för kryptering av e-postmeddelanden finns på <http://www.cert.fi/sv/aktiviteter/kontaktuppgifter/pgpnycklar.html>.

Telefon: 09 6966 510

Telefax: 09 6966 515

Postadress:
Kommunikationsverket
CERT-FI
PB 313
00181 Helsingfors

4 ÖVRIGA REKOMMENDATIONER

4.1 Rekommendation om samarbete vid kränkningar av informationssäkerhet

Kommunikationsverket rekommenderar att teleföretagen samarbetar intensivt med varandra och med Kommunikationsverkets CERT-FI-enhet i syfte att utreda informationssäkerhetskränkningar och hot mot sådana.

Det rekommenderas också att teleföretagets enheter som ansvarar för utredningen av näthantering och informationssäkerhetskränkningar underrättar andra teleföretag om sådana kränkningar och hot som påverkar eller kan påverka ett annat teleföretags kommunikationsnät eller -tjänst.

4.2 Rekommendation om att underrätta Kommunikationsverket om situationer som hänför sig till informationssäkerhet

Kommunikationsverket rekommenderar att aktörerna efter gottfinnande underrättar CERT-FI också om informationssäkerhetskränkningar och -hot som är av mindre betydelse. Uppgifterna bidrar till att skapa en lägesbild av den nationella informationssäkerheten och hjälper CERT-FI att utveckla sina tjänster som allt bättre tillgodoser aktörernas behov.

4.3 Rekommendation om att underrätta om kränkningar mot andra än teleföretag

Kommunikationsverket rekommenderar att också andra aktörer än teleföretag underrättar Kommunikationsverkets CERT-FI-enhet om de blivit utsatta för informationssäkerhetskränkningar och -hot. CERT-FI kan bland annat stöda och bistå en aktör som drabbats av kränkningen vid återhämtning och behövliga motåtgärder. CERT-FI har dessutom ett mycket omfattande internationellt samarbetsnätverk som möjliggör ett snabbt och effektivt ingripande också på internationell nivå.

5 REFERENSLISTA

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

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

<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)

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

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

[3] Strafflagen (39/1889 jämte ändringar), uppdaterad version:

<http://www.finlex.fi/sv/laki/ajantasa/1889/18890039001>

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

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

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

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

<http://www.ficora.fi/attachments/suomiry/5AWLwAxxQ/Viestintavirasto11A2008M.pdf>

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

[6] Kommunikationsverkets föreskrift 13 A/2008 M om Internetförbindelsetjänsternas informationssäkerhet och funktionsduglighet

<http://www.ficora.fi/attachments/suomiry/5AWLt8K4m/Viestintavirasto13A2008M.pdf>

<http://www.ficora.fi/attachments/ruotsiav/5B36zJiZG/Kommunikationsverket13A2008M.pdf>

[7] Kommunikationsverkets föreskrift 47 C/2009 M om informationssäkerhet hos teleföretag

<http://www.ficora.fi/attachments/suomiry/5jR9D3dp3/Viestintavirasto47C2009M.pdf>

<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/suomiry/5kfMxhxej/Viestintavirasto572009M.pdf>

<http://www.ficora.fi/attachments/ruotsiav/5kfLA59Nj/Kommunikationsverket572009M.pdf>

[9] Lagen om offentlighet i myndigheternas verksamhet (621/1999 jämte ändringar), uppdaterad version:

<http://www.finlex.fi/fi/laki/ajantasa/1999/19990621>

<http://www.finlex.fi/sv/laki/ajantasa/1999/19990621>