Datum 2015-12-16
Vår referens Dnr: 14-11014
Aktbilaga 20

Nätsäkerhetsavdelningen
Peder Cristvall
08-6785529
peder.cristvall@pts.se

Telenor Sverige AB

Säkerhetsbrister i kundplacerad utrustning

Saken

Tillsyn avseende vidtagande av lämpliga tekniska och organisatoriska åtgärder för att säkerställa skyddet av uppgifter som behandlas i samband med tillhandahållande av elektroniska kommunikationstjänster.

Post- och telestyrelsens avgörande

Post- och telestyrelsen (PTS) avskriver ärendet från vidare handläggning.

Bakgrund

PTS uppmärksammades på att det kunde föreligga säkerhetsbrister i samband med tillhandahållande av elektroniska kommunikationstjänster i den verksamhet som Telenor Sverige AB (Telenor) bedriver i Bredbandsbolaget. Enligt uppgifter i DN den 29 oktober 2014 skulle av Bredbandsbolaget tillhandahållna modem vara behäftade med säkerhetsbrister vilka kunde möjliggöra att internetuppkopplingar kapades, vilket i sin tur skulle kunna möjliggöra avlyssning.

Mot bakgrund av denna och tillkommande information har PTS beslutat att inleda tillsyn mot Telenor.

Inom ramen för tillsynen har PTS den 30 oktober 2014 begärt upplysningar angående de aktuella modemen och Telenors pågående arbete med att komma tillrätta med eventuella säkerhetsbrister. Den 14 november 2014 har PTS begärt kompletterande upplysningar. PTS och Telenor har härefter haft ett möte den 8 december 2014 vid vilket Telenor lämnat en utförligare redovisning av sina bedömningar och vidtagna åtgärder för PTS. PTS har härefter begärt

kompletterande upplysningar den 10 december 2014 respektive den 1 juni 2015. Den 11 juni 2015 har Telenor, vid möte med PTS, visat upp och beskrivit en del av den aktuella kundutrustningen och demonstrerat de tekniska system som används i samband med felsökning i kundplacerad utrustning.

Telenor har sammanfattningsvis anfört följande.

Telenor tillhandahåller tre olika modem av märket ZyXel för fast bredband till slutkunder under varumärken Bredbandsbolaget och Glocalnet. De uppgifter som standardmässigt finns lagrade i dessa enheter är konfigurationsdata för dels anslutningen till operatörsnätet, dels för kundens lokala nätverk.

Telenor har genomfört en grundlig testning av samtliga modeller av kundplacerad utrustning som distribuerats till kunderna. Telenor har identifierat ett antal sårbarheter som innebär att det funnits en teoretisk möjlighet för obehöriga att via administrationsgränssnittet ändra inställningar i modemet alternativt installera egen programvara på modemet.

För att åtgärda säkerhetsbrister har Telenor genomfört en programuppdatering av samtliga uppkopplade modem den 30 oktober 2014. Programuppdateringen åtgärdade de då identifierade säkerhetsbristerna men begränsade samtidigt användarnas möjligheter att göra egna inställningar i modemen. Kunderna hänvisades därför till kundservice för att ändra inställningar i sina modem. De kunder som identifierats med andra DNS-inställningar än standardkonfigurationen, eller med en konfiguration som inte uppfyllt erkända branschstandarder, har kontaktats och modemen har, om kund så önskat, nollställts. För ett fåtal kunder som inte varit nåbara trots upprepade kontaktförsök har en nollställning av modemen genomförts. Från Telenors sida har såväl teknisk personal som kundservice- och marknadspersonal från berörda affärsområden deltagit i hanteringen av incidenten. Säkerhetsfunktionen har representerats av Telenors Chief Information Security Officer (CISO).

Telenor har kunnat se att ett begränsat antal modem haft avvikande DNS-inställningar, d.v.s. DNS som inte räknas som branschstandard. Detta är dock inte liktydigt med att modemen har manipulerats av obehöriga. Dialog har skett med kunder med avvikande DNS-inställning för att säkerställa att de inte utsatts för obehörigt intrång. Telenor har inte kunnat konstatera intrång i något fall.

Som en långsiktig lösning har tillsammans med tillverkaren utvecklats en uppdaterad mjukvara och de säkerhetsmässigt bristfälliga konfigurationsinställningarna har förändrats så att den sammantagna säkerhetsnivån blivit god samtidigt som önskade användarkonfigurationer återställts. Ny mjukvara som permanent åtgärdar identifierade sårbarheter har tagits fram, granskats och funktionstestats samt installerats, under december 2014 för vissa modemtyper respektive november 2015 för resterande modem.

På kompletterande frågor från PTS har Telenor vidare sammanfattningsvis uppgett följande.

När det gäller typer av kundplacerad utrustning så kan deras abonnenter, beroende på typen av abonnemang, bl. a. erhålla mobiltelefoner, surfplattor, bärbara datorer, set top-boxar för TV-tjänst och modem och routrar för bredbandstjänst. Enbart i få fall är den tillhandahållna utrustningen proprietär, vilket innebär att det i många fall går att ansluta annan utrustning som uppfyller givna standarder. Internet och telefoni levereras i de flesta fall i en integrerad utrustning men de har även leverans av enbart telefoni utan internet. TV-tjänsten levereras via separat enhet som oftast ansluts bakom utrustningen för internet och telefoni. För bredbandstjänst tillhandahåller Telenor utrustning för anslutning till internet, telefoni (VoIP) samt TV (IPTV).

Vad gäller rutiner, innan en ny mjuk- eller hårdvara lanseras, så sker en testning och genomlysning som utförs av ett externt säkerhetsföretag. Det företag de anlitar har mycket goda kunskaper inom säkerhetsområdet för IT-utrustning och då speciellt penetrationstester. Innan lansering av ny kundplacerad utrustning samt innan uppdatering av mjukvara i befintlig kundplacerad utrustning granskas den aktuella produkten. Varje rapport från en sådan granskning består bland annat av en sårbarhetsanalys där eventuella sårbarheter för både Telenor och slutkunden identifieras och klassificeras. Identifierade risker diskuteras med leverantör av kundutrustning och parterna enas om hur sårbarheterna adresseras och när. När ny mjukvara eller konfiguration har tagits fram av leverantör för att åtgärda sårbarheter gör det externa säkerhetsföretaget om granskningen och en ny rapport lämnas för att bekräfta åtgärdade punkter. Någon övergripande generell risk- och sårbarhetsanalys för kundplacerad konsumentutrustning har dock historiskt inte genomförts. Däremot finns i Telenors övergripande risk- och sårbarhetsanalyser tankar och funderingar över hur denna utrustning ska hanteras och hur relaterade tjänster ska göras attraktiva och tillräckligt säkra.

När det gäller rutiner om tilldelning av behörigheter att logga in på modemen anser Telenor att det är viktigt att göra en tydlig distinktion mellan fyra kategorier av behörigheter. Behörighet att ansluta trådlöst till det av

utrustningen trådlösa nätet ges till den (kund) som har eller ges tillgång till SSID och WPA-nyckel. Vidare ges behörighet till kund att ansluta till ett begränsat administrationsgränssnitt via webbläsare. Behörighet att logga in ges vidare till supportpersonal i kundserservice och personal i drift-/utvecklingsorganisationen.

I samband med händelsen har Telenor lämnat löpande information om sårbarheten och vidtagna åtgärder med start den 29 oktober 2014. Informationen har sedan kontinuerligt uppdaterats under de följande veckorna. Telenor har även informerat via kundtjänst och media och via sina kanaler på sociala medier. Kundbrev med information om hur man som abonnent återställer modemet har skickats till samtliga abonnenter med modem som behövde uppdateras för att få senaste konfigurationen. På bredbandsbolaget.se finns en guide om hur abonnenten gör egna konfigureringar i modemet.

Telenor har vidare redogjort för den kravställning som sker gentemot leverantörer vad gäller säkerheten för kundplacerad utrustning och de rutiner och kontroller som görs för att upptäcka fall där säkerhetsbrister utnyttjats av obehöriga.

Skäl

Tillämpliga bestämmelser

Enligt 6 kap. 3 § i lagen (2003:389) om elektronisk kommunikation (LEK) ska den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att uppgifter som behandlas i samband med tillhandahållande av tjänsten skyddas. Den som tillhandahåller ett allmänt kommunikationsnät ska vidta de åtgärder som är nödvändiga för att upprätthålla detta skydd i nätet. Åtgärderna ska vara ägnade att säkerställa en säkerhetsnivå, som med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för integritetsincidenter. Av PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1)[1] framgår bland annat följande:

Tjänstetillhandahållarens säkerhetsarbete avseende behandlade uppgifter ska enligt 3 § bedrivas långsiktigt, kontinuerligt och systematiskt och det ska finnas en tydlig rollfördelning med särskilt utpekade ansvariga. Rutiner, processer och rollfördelning ska dokumenteras.

Tjänstetillhandahållaren ska enligt 4 § identifiera informationsbehandlings-tillgångar där behandlade uppgifter förekommer och föra en förteckning över

[1] Post- och telestyrelsens föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter, PTSFS 2014:1.

dessa. Tjänstetillhandahållaren ska analysera riskerna för att integritetsincidenter inträffar för de identifierade informationsbehandlingstillgångarna. Riskanalyserna ska dokumenteras och följas upp årligen och vid behov. Tjänstetillhandahållaren ska vidta föreskrivna skyddsåtgärder samt andra nödvändiga skyddsåtgärder, på den nivå som är lämplig för att hantera de identifierade riskerna. Vidtagna skyddsåtgärder samt tjänstetillhandahållarens bedömningar av lämplig nivå ska dokumenteras och följas upp årligen och vid behov.

Tjänstetillhandahållaren ska enligt 5 § säkerställa att åtkomst till behandlade uppgifter endast ges till den som
1. behöver det för att utföra sina arbetsuppgifter,
2. har relevant utbildning med hänsyn till de uppgifter denne hanterar,
3. har upplysts om tystnadsplikten i 6 kap. 20 – 21 §§ lagen (2003:389) om elektronisk kommunikation.

Tjänstetillhandahållaren ska enligt 6 § tilldela behörighet i enlighet med vad som föreskrivs i 5 §. Tjänstetillhandahållaren ska ha dokumenterade rutiner för tilldelning, ändring och uppföljning av behörigheter. Uppföljning av tilldelade behörigheter ska ske årligen.

Tjänstetillhandahållaren ska vidare ha system för identitets- och åtkomsthantering som säkerställer att åtkomst endast medges i enlighet med tilldelade behörigheter.

Tjänstetillhandahållaren ska enligt 7 § dokumentera (logga) all läsning, kopiering, ändring och utplåning av behandlade uppgifter samt åtkomst till de system som används för behandling av sådana uppgifter. Loggning ska ske på ett sådant sätt att det går att se vem som har vidtagit vilken åtgärd med vilka uppgifter och vid vilken tidpunkt. Tjänstetillhandahållaren ska systematiskt och återkommande kontrollera loggarna. Kontrollerna får avgränsas till att omfatta utvalda behandlingar under begränsade tidsperioder, om kostnaderna för kontrollen motiverar en sådan avgränsning. Tjänstetillhandahållaren ska dokumentera genomförda kontroller av loggar. Vid misstanke om att en integritetsincident har inträffat ska relevanta loggar alltid kontrolleras. Tjänstetillhandahållaren ska ha dokumenterade rutiner för kontroll av loggar.

Tjänstetillhandahållaren ska enligt 10 § ha dokumenterade rutiner för identifiering, intern rapportering, hantering och uppföljning av integritetsincidenter. Rutinerna ska säkerställa
1. att samtliga uppgifter i 11 § förs in i den förteckning som tjänstetillhandahållaren ska föra enligt 6 kap. 4 b § lagen (2003:389) om elektronisk kommunikation,

2. att inträffade integritetsincidenter och dess orsaker beaktas vid genomgång av riskanalyser i enlighet med 4 §, och
3. att skyddsåtgärder vidtas för att undvika liknande integritetsincidenter.

Tillsynsmyndigheten ska enligt 7 kap. 1 § LEK utöva tillsyn över bland annat efterlevnaden av lagen.

PTS bedömning

Den föreliggande tillsynen har föranletts av brister som uppmärkammats avseende tre olika modem för fast bredband till slutkunder som tillhandahålls i den verksamhet Telenor bedriver i Bredbandsbolaget. Det har funnits risk att de uppmärksammade bristerna skulle utnyttjas av obehöriga för att via ett administrationsgränssnitt ändra inställningar eller installera egen programvara på modemen och därigenom kunna ta del av innehållet och kunnat påverka den kommunikation som förmedlats. Telenor har dock inte kunnat fastställa att sårbarheterna har utnyttjats i något fall.

PTS kan konstatera att de aktuella modemen för abonnenten utgör en förutsättning för att kunna ta del av en eller flera av de tjänster som tillhandahålls av Telenor. Såväl IP-TV som IP-telefoni (i vissa fall) ska enligt instruktionerna från Telenor kopplas in via modemen. Via modemen tillhandahålls även trådbunden eller trådlös internetuppkoppling. Användare har dessutom möjlighet att koppla in ytterligare utrustning i form av t.ex. egna routrar.

När det gäller inställningar och användningen av utrustningen kan konstateras att kunderna får behörighet och möjlighet att ansluta till utrustningen via ett begränsat administrationsgränssnitt. Genom anslutningen ges kunderna möjlighet att i viss grad anpassa utrustningen, till exempel genom att sätta egna lösenord.

Telenors personal kan genomföra fjärrinloggning i samband med supportärenden. Detta innebär att Telenor har kontroll av delar av utrustningen som kunden inte råder över eller har möjlighet att påverka. Med hjälp av denna kontroll kan Telenor genomföra nödvändiga uppgraderingar och stödja sina kunder i samband med problem relaterade till den aktuella utrustningen.

Av 6 kap 3 § LEK följer att den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att uppgifter som behandlas *i samband med* tillhandahållandet av tjänsten skyddas. En fråga i detta ärende är hur långt detta ansvar sträcker sig när det gäller kundplacerad utrustning. Som framgår

ovan förutsätts kunderna i normalfallet använda den aktuella kundplacerade utrustningen för åtkomst till Telenors kommunikationstjänster. Telenor har dessutom uteslutande kontroll vad gäller hanteringen av väsentliga inställningar. I och med att det endast är Telenor som kan göra ändringar i dessa inställningar får Telenor anses förfoga över modemen i dessa delar. Mot bakgrund av dessa omständigheter bedömer PTS att den aktuella utrustningen utgör en tillgång som används av Telenor för att tillhandahålla elektroniska kommunikationstjänster. Den omfattas därmed av bestämmelsen i 6 kap 3 § LEK. Eftersom utrustningen innehåller uppgifter knutna till vissa abonnemang och därtill används för att förmedla abonnenternas trafik får den anses utgöra en sådan informationsbehandlingstillgång som regleras i PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1).

Nedan följer de bedömningar PTS gör vad gäller Telenors åtgärder beträffande de aktuella modemen i förhållande till tillämpliga krav som de framgår av PTS föreskrifter.

Säkerhetsarbete i enlighet med 3 § i PTSFS 2014:1

I föreliggande ärende framgår att Telenor uppmärksammades på de aktuella sårbarheterna via ett e-postmeddelande med anledning av en publicering som skulle ske i en av Sveriges större morgontidningar. För att hantera incidenten har såväl teknisk personal som kundservice- och marknadspersonal från berörda affärsområden deltagit i hanteringen av incidenten. Säkerhetsfunktionen har representerats av Telenors CISO.

Kravet i 3 § föreskrifterna på säkerhetsarbete syftar bland annat till att minimera risker för otillåtna ingrepp i abonnenters och användares personliga integritet och att öka verksamhetens förmåga att upptäcka och hantera de incidenter som inträffar. Telenor har beskrivit sitt övergripande säkerhetsarbete bland annat inom ramen för ett annat tillsynsärende hos PTS (Dnr 15-4419). Av redovisningen i det ärendet framgår att Telenor tillämpar rutiner för upptäckt av integritetsincidenter och har en organisation som styrs av en intern policy med särskilt utpekade ansvariga för att kunna upptäcka och hantera inträffade integritetsincidenter.

Telenor har också beskrivit ett antal åtgärder som vidtagits för att informera kunderna och för att uppgradera mjukvaran m.m. med anledning av uppmärksammade sårbarheter. PTS noterar att säkerhetsarbetet huvudsakligen varit av reaktiv karaktär med anledning av de säkerhetsbrister som uppmärksammats i detta ärende och vill i detta sammanhang betona vikten av ett kontinuerligt förebyggande säkerhetsarbete för att så långt som möjligt undvika incidenter och för att kunna hantera risker på ett tidigt stadium. Den kundplacerade utrustningen utgör sådana informationsbehandlingstillgångar

som regleras i PTS föreskrifter och det är viktigt att det övergripande säkerhetsarbetet även omfattar dessa.

Med detta påpekande lämnar PTS frågan hur Telenor efterlever den aktuella bestämmelsen utan vidare åtgärd. PTS kan dock återkomma till frågan i framtida tillsynsärenden.

Identifikation av informationsbehandlingstillgångar, genomförande av riskanalyser och vidtagande av skyddsåtgärder i enlighet med 4§ PTSFS 2014:1

PTS har ovan konstaterat att modem får anses utgöra sådana informationsbehandlingstillgångar som omfattas av kraven i PTSFS 2014:1. Av 4 § framgår att tjänstetillhandahållaren ska *identifiera sina informationsbehandlingstillgångar och föra en förteckning över dessa*. En grundläggande förutsättning för att en tjänstetillhandahållare ska kunna vidta lämpliga åtgärder, upprätthålla en lämplig skyddsnivå och följa upp sitt säkerhetsarbete är att denne har en samlad bild över de informationsbehandlingstillgångar där uppgifter behandlas i samband med tillhandahållande av elektroniska kommunikationstjänster.

PTS föreskrifter reglerar inte särskilt i vilken form förteckningen av informationsbehandlingstillgångar ska föras. Syftet med förteckningen är dock att tjänstetillhandahållaren bland annat ska få en överblick och kunna planera sitt arbete med t.ex. riskanalyser. I samband med upptäckta sårbarheter eller inträffade incidenter kan förteckningen också användas för att t.ex. underlätta programuppdateringar i kundutrustningen och för att kontakta de abonnenter som är berörda.

PTS har valt att inom ramen för denna tillsyn inte närmare granska hur förteckningen förs eller dess innehåll. PTS har dock för avsikt att återkomma till frågan om förteckningen över informationsbehandlingstillgångar i kommande tillsynsarbete.

PTS föreskrifter anger vidare att en kartläggning ska ske av riskerna för att integritetsincidenter inträffar för identifierade informationsbehandlings-tillgångar eller grupper av tillgångar. Den genomförda riskanalysen styr omfattningen av de skyddsåtgärder som vidtas beträffande de aktuella informationsbehandlingstillgångarna. En sådan analys ska dokumenteras, liksom de säkerhetsåtgärder som behöver vidtas för att hantera de identifierade riskerna.

PTS kan konstatera att Telenor genomför en teknisk analys som är inriktad mot risker hänförliga till de olika typer av modem som tillhandahålls. Eftersom nya sårbarheter kan uppkomma eller upptäckas efterhand är regelbundna riskanalyser nödvändiga för att kunna hantera nya och förändrade risker. Enligt föreskrifterna ska genomförda riskanalyser följas upp minst en gång per år.

Det är också viktigt att ha en löpande omvärldsbevakning för att få kännedom eventuella nya sårbarheter så att en bedömning kan göras om det finns behov av förnyade riskanalyser eller andra åtgärder. Telenor har i ärendet bland annat uppgett att det säkerhetsarbete som bedrivits med leverantören och ett externt säkerhetsföretag för att åtgärda i ärendet funna brister kommer att permanentas för att säkra att inte nya brister uppstår.

När det gäller de aktuella modemen har Telenor uppgett att någon övergripande och generell risk- och sårbarhetsanalys för kundplacerad konsumentutrustning inte har genomförts. Däremot finns i bolagets övergripande risk- och sårbarhetsanalyser tankar och funderingar över hur denna utrustning ska hanteras och hur relaterade tjänster ska göras attraktiva och tillräckligt säkra. För de specifika enheterna görs en djupare teknisk sårbarhetsanalys och lämpliga åtgärder för att hantera identifierade risker diskuteras med leverantörer av kundutrustningen.

PTS kan konstatera att det ovan beskrivna arbetet huvudsakligen står i överensstämmelse med PTS föreskrifter. Telenor har dock uppgett att man inte genomfört någon övergripande och generell sårbarhetsanalys för kundplacerad konsumentutrustning. PTS anser att även en övergripande, mer generell riskanalys, är nödvändig för att beakta eventuella risker som inte är direkt relaterade till modemen och deras hård- och mjukvara. En sådan analys skulle t.ex. kunna omfatta hanteringen av lösenord och överväganden vad gäller abonnenternas möjligheter att göra egna inställningar i modemen.

Åtkomst till uppgifter i enlighet med 5 § och tilldelning av behörighet i enlighet med 6 § PTSFS 2014:1

Syftet med bestämmelserna är att tillgodose skyddet av behandlade uppgifter genom att förhindra obehörig användning eller åtkomst till behandlade uppgifter genom regler för åtkomst- och behörighetshantering.

Bestämmelserna gäller enligt PTS bedömning för tjänstetillhandahållarnas egen personal (och personal hos underleverantörer). Genom bestämmelserna begränsas åtkomstmöjligheterna till känsliga uppgifter, så att endast den personal som behöver dessa för att utföra sina arbetsuppgifter får tillgång till uppgifterna. Vidare bör tillförsäkras att personalen har god kännedom om reglerna om tystnadsplikt och har en relevant utbildning så att den vet när och

hur behandlade uppgifter får behandlas, kan se tecken på att incident har inträffat och kan bedöma tänkbara konsekvenser av inträffade incidenter m.m. Av det allmänna rådet till 5 § föreskrifterna framgår att en relevant utbildning bör innefatta information som ger personalen kunskap att upptäcka, bedöma och rapportera integritetsincidenter.

PTS kan konstatera att såväl support- som driftsärenden kräver åtkomst till vissa av de uppgifter som behandlas i modemen. Telenor har beskrivit att man tilldelar supportpersonal i kundservice och teknisk personal i drift-/utvecklingsorganisationen behörighet att genomföra fjärrinloggning. Båda kategorierna av personal utgör en begränsad andel av Telenors (eller underleverantörs) personal och tilldelas behörighet med utgångspunkt i behovet av att ta del av uppgifter för att kunna vidta nödvändiga åtgärder för drift och kundstöd.

Utifrån de uppgifter Telenor lämnat gör PTS bedömningen att behörighet till åtkomst till modemen endast ges till de som behöver det för att utföra sina arbetsuppgifter. PTS har dock inte inom ramen för detta tillsynsärende närmare granskat de system för identitets- och åtkomsthantering som är nödvändiga för att säkerställa att åtkomst endast medges i enlighet med tilldelade behörigheter.

PTS gör bedömningen att bestämmelserna inte är avsedda att reglera villkoren för abonnenternas användning av kundplacerad utrustning. Detta medför att bestämmelserna inte hindrar att abonnenter ges möjlighet att ändra vissa inställningar i t.ex. modem för att anpassa dessa till sina behov.

7 § loggning

Av 7 § framgår att tjänstetillhandahållare ska logga all behandling som sker av uppgifter i och åtkomst till system som används för behandling av uppgifter. Loggarna ska återkommande kontrolleras och dokumentation ska ske av genomförda kontroller.

PTS gör bedömningen att de åtgärder med modemen som genomförs av supportpersonal i kundservice och av teknisk personal i drift/utvecklingsorganisationen omfattas av skyldigheten att logga utförda behandlingar. PTS kan konstatera att loggning sker av berörd personals åtgärder. PTS har dock inte särskilt granskat loggar eller utförda kontroller av dessa i detta ärende.

Samlad bedömning

Mot bakgrund av de åtgärder Telenor har genomfört och redovisat i ärendet för att komma till rätta med de uppmärksammade säkerhetsbristerna och med de

påpekanden PTS har gjort ovan, kan myndigheten konstatera att det saknas anledning att vidta ytterligare åtgärder i ärendet. Ärendet ska därför avskrivas från vidare handläggning.

Beslutet har fattats av enhetschefen Patrik Bystedt. Föredragande har varit juristen Peder Cristvall.