Vår referens: 23-978, **Aktbilaga:** 12

WhatsApp Ireland Limited, med säte i Irland, org. nr 607470

Ombud: Cirio Advokatbyrå AB, org. Nr 556953-0008

Underrättelse om misstanke om bristande efterlevnad av bestämmelser om rapportering av säkerhetsincidenter

Saken

Underrättelse enligt 11 kap. 5 § lagen (2022:482) om elektronisk kommunikation (LEK)

Post- och telestyrelsens underrättelse

WhatsApp Ireland Limited (WhatsApp) underrättas om Post- och telestyrelsens (PTS) misstanke att WhatsApp inte efterlever skyldigheten att rapportera säkerhetsincidenter till PTS enligt 8 kap. 3 § LEK samt 17 kap. 1 - 5 §§ i Post- och telestyrelsens föreskrifter och allmänna råd om säkerhet i nät och tjänster, PTSFS 2022:11 (PTS säkerhetsföreskrifter) genom att inte rapportera det avbrott i tjänsten WhatsApp, som inträffade den 25 oktober 2022 som en säkerhetsincident. Det finns brister i den information WhatsApp har lämnat till PTS för kännedom. Uppgiftslämnandet är inte komplett utifrån de regler som gäller för rapportering av säkerhetsincidenter och har inte skett inom den föreskrivna tiden för rapportering av säkerhetsincidenter.

För att efterleva gällande regler ska WhatsApp inkomma med de ytterligare uppgifter som anges i punktuppställningen under PTS bedömning i denna underrättelse i enlighet med de krav som ställs i 17 kap. 3 och 4 §§ i PTS säkerhetsföreskrifter.

WhatsApp ges tillfälle att yttra sig över denna underrättelse **senast den 26 april 2023**.

I yttrandet bör WhatsApp ange vilka åtgärder som företaget vidtagit eller avser att vidta med anledning av underrättelsen samt när dessa beräknas vara vidtagna.

Om WhatsApp inte inkommer med yttrande kan PTS komma att fatta beslut på det underlag som står till myndighetens förfogande.

Post- och telestyrelsen
Postadress: Box 5398, 102 49 Stockholm
Besöksadress: Valhallavägen 117 A
Telefon: 08-678 55 00
E-post: pts@pts.se
www.pts.se

Bakgrund

Inträffad incident i oktober 2022

Den 27 oktober 2022 kontaktade PTS WhatsApps svenska ombud efter att PTS fått kännedom om en inträffad händelse (avbrott) i tjänsten WhatsApp den 25 oktober 2022. PTS ställde bl.a. frågan om bolaget har för avsikt att rapportera händelsen till PTS som en säkerhetsincident eftersom avbrottet medfört betydande påverkan på bolagets tjänster. Vidare upplyste PTS om att sådana säkerhetsincidenter som har haft en betydande påverkan på WhatsApps tjänster ska rapporteras till PTS, bl.a. om svenska användare har drabbats i viss utsträckning. PTS hänvisade specifikt till reglerna i 1 kap 7 § LEK (definitionen av säkerhetsincident) och i 8 kap 3 § LEK (övergripande rapporteringsplikt) tillsammans med 17 kap. i PTS säkerhetsföreskrifter.

Den 28 oktober 2022 inkom WhatsApp, via det svenska ombudet, med svar på PTS frågor. I svaret till PTS uppgav bolaget bl.a. att WhatsApp hade ett serviceavbrott den 25 oktober 2022, ungefär kl. 08:00 (GMT) och att WhatsApps meddelande- och samtalstjänster var helt återställda runt kl. 10:47 GMT (trafik på 100 %). Vidare uppgav WhatsApp att bolaget hade kommit fram till att den aktuella incidenten inte var en anmälningspliktig säkerhetsincident enligt definitionen i kodexen[1] men att WhatsApp ansåg att det var lämpligt att ge PTS en uppdatering för kännedom.

Den 3 november 2022 upplyste PTS WhatsApp om att bolaget behöver tillämpa svenska regler i LEK och PTS säkerhetsföreskrifter när WhatsApp gör bedömningen om en incident är rapporteringspliktig i Sverige. PTS hänvisade bl.a. till bestämmelser om tröskelvärden för rapportering i PTS säkerhetsföreskrifter. PTS ställde frågan hur WhatsApps bedömning av rapporteringsplikten blir när den istället sker utifrån de gällande svenska reglerna.

Den 18 november 2022 återkom WhatsApp via sitt svenska ombud med bl.a. en skrivelse med en beskrivning av händelseförloppet under den aktuella incidenten samt WhatsApps bedömning av definitioner i kodexen. I skrivelsen uppger WhatsApp bl.a. att det aktuella avbrottet innebar att bolagets tjänster tillfälligt var otillgängliga för användare mellan ca kl. 8.00 (GMT) till kl. 10.47 (GMT), men att WhatsApp återställde meddelande- och samtalstjänster cirka kl. 10.17 (GMT). Vidare framgår av skrivelsen att WhatsApp uppskattar att cirka 1,1 miljoner WhatsApp-användare i Sverige påverkades av incidenten.

[1] Europaparlamentets och rådets direktiv (EU) 2018/1972
av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation.

WhatsApp redogör för sin syn på rapporteringsskyldigheten enligt kodexen

I skrivelsen till PTS redogör WhatsApp även för sin syn på rapporteringsskyldigheten och framför att det enligt kodexen inte finns någon rapporteringsskyldighet för den aktuella incidenten. WhatsApp anger bl.a. följande.

Genom artikel 1.1 i kodexen harmoniseras definitionen av ”säkerhetsincident” inom EU. WhatsApp uppger vidare att när definitionen av ”säkerhetsincident” i artikel 2.42 i kodexen läses tillsammans med definitionen av ”säkerhet i nät och tjänster” i artikel 2.21 i kodexen så utgör ”säkerhetsincident” därför en händelse som har en faktisk negativ effekt på nätens och tjänsternas förmåga att vid en viss tillförlitlighetsnivå, motstå åtgärder som undergräver tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos dessa nät och tjänster, av lagrade eller överförda eller bearbetade data, eller av de relaterade tjänster som erbjuds av eller är tillgängliga via, dessa nätverk eller tjänster.

WhatsApp konstaterar därefter att vad gäller den aktuella händelsen, så ledde vissa omständigheter till avbrott i WhatsApps tjänster, men att de underliggande näten och tjänsterna fortsatt hade förmåga att upptäcka, förebygga och avhjälpa potentiella åtgärder som kan påverka sådana nät och tjänster. Vad gäller tillgänglighet är avbrott respektive händelser med en faktisk negativ effekt på förmågan att motstå avbrott ovillkorligen skilda från varandra och olika.

WhatsApp uppger vidare att det aktuella avbrottet inte i sig ska tolkas som att det automatiskt innebar att tjänsternas förmåga att motstå åtgärder som kan undergräva tillgängligheten (eller riktighet, integritet eller konfidentialitet) för sådana tjänster var påverkad. I annat fall skulle regeln konsumera sig själv genom att varje avbrott, oavsett anledning, skulle utgöra en säkerhetsincident utan att hänsyn tas till tjänstens förmåga att motstå avbrott.

I skrivelsen uppger WhatsApp sammanfattningsvis att det inte inträffade någon händelse som minskade tjänstens förmåga att motstå sådana åtgärder och därmed inträffade ingen säkerhetsincident enligt kodexens mening.

Skäl

Tillämpliga bestämmelser

I 11 kap. 5 § LEK anges att om PTS misstänker att den som bedriver verksamhet enligt denna lag inte följer lagen eller de beslut om skyldigheter, åtaganden eller villkor som har meddelats med stöd av lagen eller de föreskrifter som har meddelats i anslutning till lagen, ska

myndigheten underrätta den som bedriver verksamheten om misstanken och ge denne möjlighet att yttra sig inom skälig tid. Detta gäller även när PTS misstänker att någon inte följer en genomförandeåtgärd som avses i 11 kap. 1 § andra stycket LEK eller inte använder en radiosändare i den utsträckning som villkoren medger.

Av 1 kap. 7 § LEK framgår att med säkerhetsincident avses en händelse med en faktisk negativ inverkan på tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst, hos lagrade, överförda eller behandlade uppgifter eller hos de närliggande tjänster som erbjuds genom eller är tillgängliga via dessa elektroniska kommunikationsnät eller elektroniska kommunikationstjänster, eller på förmågan att motstå sådana händelser.

Av 8 kap. 3 § LEK framgår bl.a. att den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst utan onödigt dröjsmål ska rapportera säkerhetsincidenter till PTS som har haft en betydande påverkan på nät och tjänster.

Av bestämmelsens andra stycke framgår att PTS har bemyndiganden att meddela ytterligare föreskrifter om rapportering av säkerhetsincidenterna och föreskrifter om undantag från rapporteringsskyldigheten.

Av 17 kap. 1 § PTS säkerhetsföreskrifter framgår att tillhandahållaren bl.a. ska rapportera sådana säkerhetsincidenter som anges i 5 §.

Av 17 kap. 2 § PTS säkerhetsföreskrifter framgår att tillhandahållaren vid incidentrapportering ska lämna en inledande och en kompletterande rapport.

Av 17 kap. 3 § PTS säkerhetsföreskrifter framgår att den inledande rapporten ska vara Post- och telestyrelsen till handa inom 72 timmar från det att säkerhetsincidenten upptäcktes och att den ska innehålla uppgifter om

1. när säkerhetsincidenten inträffade,
2. hur länge säkerhetsincidenten har pågått,
3. antal aktiva anslutningar eller användare som har drabbats av säkerhetsincidenten,
4. berört geografiskt område, i de fall det är relevant,
5. vilka säkerhetsaspekter (tillgänglighet, autenticitet, riktighet eller konfidentialitet) som har berörts av säkerhetsincidenten,
6. vilka kommunikationsnät, kommunikationstjänster, lagrade, överförda eller behandlade uppgifter eller närliggande tjänster som har berörts av säkerhetsincidenten,
7. säkerhetsincidentens påverkan på kommunikationsnätet eller kommunikationstjänsten eller påverkan på funktioner i samhället,
8. tillhandahållarens preliminära bedömning av orsaken till säkerhetsincidenten,
9. hur säkerhetsincidenten har påverkat berörda aktiva anslutningar eller användare i Sverige,

10. huruvida säkerhetsincidenten har medfört begränsningar i möjligheten till nödkommunikation via det kommunikationsnät eller den kommunikationstjänst som berörts av säkerhetsincidenten, och
11. tillhandahållarens kontaktuppgifter och referensnummer för ärendet.

Allmänt råd till 3 §

Tillhandahållaren bör göra en uppskattning av tidpunkten för när säkerhetsincidenten har inträffat i de fall en exakt tidpunkt inte kan fastställas med stöd av system för övervakning eller loggning. Uppskattningen bör göras med utgångspunkt från kända fakta om incidenten.

Redogörelsen enligt 3 § 6 bör innehålla såväl uppgifter om de berörda nätteknologierna som uppgift om berörda slutanvändartjänster, till exempel rösttelefoni, meddelandetjänst eller internetanslutning.

Av 17 kap. 4 § PTS säkerhetsföreskrifter framgår att den kompletterande rapporten ska vara Post- och telestyrelsen till handa inom två veckor från det att den inledande rapporten lämnades och att anstånd kan beviljas. Vidare framgår att rapporten ska innehålla uppgifter om

1. komplettering och uppdatering av uppgifterna som lämnats i den inledande rapporten,
2. orsakerna till säkerhetsincidenten,
3. vilken information som har lämnats till allmänheten och berörda personer samt vid vilken tidpunkt och på vilket sätt denna information lämnades,
4. de åtgärder som har vidtagits för att minimera effekterna av säkerhetsincidenten inför slutligt avhjälpande,
5. de åtgärder som har vidtagits för att avhjälpa de fel och brister som orsakat säkerhetsincidenten och vid vilken tidpunkt åtgärderna vidtogs,
6. de åtgärder som har vidtagits och som planeras för att undvika liknande säkerhetsincidenter samt vid vilken tidpunkt dessa åtgärder vidtogs eller när de bedöms vara genomförda, och
7. referensnummer för ärendet.

Allmänt råd till 4 §

Tillhandahållarens redogörelse för orsakerna till säkerhetsincidenten bör beskriva samtliga kända omständigheter som har eller kan ha bidragit till att incidenten inträffade.

Av 17 kap. 5 § PTS säkerhetsföreskrifter följer att säkerhetsincidenter som innebär störning eller avbrott (tillgänglighet) i tillhandahållna kommunikationsnät eller

kommunikationstjänster alltid ska rapporteras under förutsättning att vissa tröskelvärden är uppfyllda, se tabell nedan.

Tid som incidenten pågått	*Incidentens uppskattade omfattning*
≥ 1 timme	≥ 150 000 användare eller aktiva anslutningar i Sverige, ≥ 50 procent kapacitetsbortfall eller ≥ 15 000 km² sammanhängande berört område
≥ 2 timmar	≥ 30 000 användare eller aktiva anslutningar i Sverige, ≥ 30 procent kapacitetsbortfall eller ≥ 5 000 km² sammanhängande berört område
≥ 6 timmar	≥ 5 000 användare eller aktiva anslutningar i Sverige, ≥ 20 procent kapacitetsbortfall eller ≥ 2 500 km² sammanhängande berört område
≥ 24 timmar	≥ 2 000 användare eller aktiva anslutningar i Sverige, ≥ 10 procent kapacitetsbortfall eller ≥ 1 000 km² sammanhängande berört område

Allmänt råd till 5 §

Berört område för kommunikationstjänster som tillhandahålls över mobila nätanslutningar bör normalt vara det sammanlagda täckningsområdet för berörda celler eller motsvarande i mobilnätet.

Kapacitetsbortfall bör till exempel kunna beräknas som andelen berörda användare eller aktiva anslutningar i förhållande till det totala antalet användare eller aktiva anslutningar för kommunikationstjänsten, eller, andel misslyckade samtalsförsök.

PTS bedömning

WhatsApp tillhandahåller tjänster i Sverige

WhatsApp har sitt säte i Irland och erbjuder kommunikationstjänsten WhatsApp till användare i Sverige. Tjänsten är en s.k. nummeroberoende interpersonell kommunikationstjänst (NI-ICS[2]) då den möjliggör kommunikation mellan personer utan användning av nummer. I och med att tjänsten marknadsförs på svenska, har ett mycket stort antal användare i Sverige och är anpassad till svenska förhållanden bl.a. genom att

[2] Number-independent interpersonal communication services.

webbplatsen är på svenska, bedömer PTS att WhatsApp tillhandahåller tjänsten i Sverige och att bolaget ska följa svensk lagstiftning även om bolaget har sin hemvist i Irland. Tillhandahållare av nummeroberoende interpersonella kommunikationstjänster i Sverige omfattas sedan 3 juni 2022 av LEK och sedan 1 augusti 2022 av PTS säkerhetsföreskrifter, vilket innebär att dessa tillhandahållare måste följa vissa säkerhetsregler i samband med sitt tjänstetillhandahållande. WhatsApp måste exempelvis hantera risker som hotar säkerheten i nät och tjänster, vidta säkerhetsåtgärder samt rapportera säkerhetsincidenter som har haft en betydande påverkan på nät och tjänster till PTS.

WhatsApp är rapporteringsskyldigt för faktiska avbrott i tjänsten

I skrivelsen från WhatsApp som inkom till PTS den 18 november 2022 redogör bolaget för sin syn på rapporteringsskyldigheten och framför att det enligt kodexen inte finns någon rapporteringsskyldighet för den aktuella incidenten. Av skrivelsen framgår att WhatsApps ståndpunkt är att en förutsättning för rapporteringsplikt av säkerhetsincidenter är att händelsen handlar om påverkad *förmåga* att upprätthålla en viss säkerhetsnivå medan faktiska avbrott inte är rapporteringspliktiga.

Som framgår av 8 kap. 3 § LEK tillsammans med definitionen av säkerhetsincident i 1 kap. 7 § LEK ska den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst utan onödigt dröjsmål rapportera *händelser med faktisk negativ inverkan på bl.a. tillgängligheten som har haft en betydande påverkan på nät och tjänster* till PTS.

Baserat på de uppgifter WhatsApp har lämnat till PTS 28 oktober 2022 samt 18 november 2022, bedömer PTS att den beskrivna inträffade händelsen i WhatsApp-tjänsten den 25 oktober 2022 når upp till trösklarna i 17 kap. 5 § PTS säkerhetsföreskrifter eftersom avbrottet i WhatsApp-tjänsten varade i mer än två timmar och uppskattningsvis påverkade cirka 1,1 miljoner WhatsApp-användare i Sverige. Incidenten borde därmed ha rapporterats till PTS i enlighet med regelverket.

Bedömningen att en rapporteringspliktig säkerhetsincident har inträffat vid en händelse med en faktisk negativ inverkan följer även av resonemanget i förarbetena till LEK. Enligt regeringen ska definitionen av säkerhetsincident inte enbart begränsas till en händelse som bara påverkar förmågan att motstå åtgärder som undergräver tillgänglighet, riktighet etc. Den ska även omfatta en händelse med en faktisk negativ inverkan på tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst, hos lagrade, överförda eller behandlade uppgifter eller hos de närliggande tjänster som erbjuds genom eller är tillgängliga via dessa

elektroniska kommunikationsnät eller elektroniska kommunikationstjänster, eller på förmågan att motstå sådana händelser.[3]

WhatsApp är en stor tillhandahållare av kommunikationstjänster och har många användare i Sverige. Det finns därmed en risk att eventuella framtida avbrott och störningar i WhatsApp-tjänsten potentiellt kan drabba många svenska användare. Vid utebliven rapportering av faktiska säkerhetsincidenter avseende avbrott och störningar (tillgänglighet) i enlighet med PTS rapporteringströsklar finns det således risk att PTS inte får vetskap om allvarliga händelser och att PTS inte får del av viktig information kring incidenten. PTS har även en skyldighet att vidarerapportera större incidenter till ENISA varje år i enlighet med gällande EU-rättsakter.[4]

Vissa uppgifter saknas och vissa har inkommit för sent

PTS har upplyst WhatsApp om de svenska rapporteringsreglerna i samband med att PTS kontaktade bolaget 27 oktober 2022. PTS har bl.a. hänvisat till rapporteringsreglerna i LEK och i PTS säkerhetsföreskrifter samt bifogat länk till såväl PTS mall för incidentrapportering på PTS webbplats som PTS säkerhetsföreskrifter.

Den 28 oktober 2022 uppgav WhatsApp till PTS att bolaget ansåg att den aktuella incidenten inte var en anmälningspliktig säkerhetsincident enligt kodexen, men att bolaget ansåg att det var lämpligt att ge PTS en uppdatering för kännedom.

Av 17 kap. 1 § PTS säkerhetsföreskrifter framgår att vid rapportering av säkerhetsincidenter ska en inledande och en kompletterande rapport lämnas till Post- och telestyrelsen. Uppdateringen från WhatsApp den 28 oktober 2022 innehöll inte all information som krävs i samband med en inledande incidentrapportering enligt reglerna i 17 kap. 3 § säkerhetsföreskrifterna. Följande information saknades vid denna tidpunkt;

- antal aktiva anslutningar eller användare som har drabbats av säkerhetsincidenten (uppgift om detta lämnades först 18 november 2022),
- tillhandahållarens preliminära bedömning av orsaken till säkerhetsincidenten,
- hur säkerhetsincidenten har påverkat berörda aktiva anslutningar eller användare i Sverige,

[3] Prop. 2021/22:136 Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation, s. 319.

[4] ENISA står för The European Union Agency for Cybersecurity

- om säkerhetsincidenten har medfört begränsningar i möjligheten till nödkommunikation via det kommunikationsnät eller den kommunikationstjänst som berörts av säkerhetsincidenten.

I samband med att PTS den 3 november 2022 upplyste WhatsApp om att bolaget behöver tillämpa svenska regler i LEK och PTS säkerhetsföreskrifter när WhatsApp gör bedömningen om en incident är rapporteringspliktig i Sverige, hänvisade PTS återigen till PTS säkerhetsföreskrifter och bifogade en länk till dessa.

WhatsApp återkom till PTS med ytterligare information om incidenten den 18 november 2022, bl.a. med en beskrivning av händelseförloppet vid den aktuella incidenten. Denna kompletterande information kring incidenten saknade emellertid ett antal uppgifter som enligt 17 kap. 4 § PTS säkerhetsföreskrifter ska uppges i samband med kompletterande rapportering av säkerhetsincidenter. Följande information saknades;

- vilken information som har lämnats till allmänheten och berörda personer samt vid vilken tidpunkt och på vilket sätt denna information lämnades,
- de åtgärder som har vidtagits för att minimera effekterna av säkerhetsincidenten inför slutligt avhjälpande,
- de åtgärder som har vidtagits för att avhjälpa de fel och brister som orsakat säkerhetsincidenten och vid vilken tidpunkt åtgärderna vidtogs,
- de åtgärder som har vidtagits och som planeras för att undvika liknande säkerhetsincidenter samt vid vilken tidpunkt dessa åtgärder vidtogs eller när de bedöms vara genomförda.

Av 17 kap. 4 § PTS säkerhetsföreskrifter framgår vidare att den senaste tidpunkten att lämna en kompletterande rapport till PTS är två veckor från att en inledande rapportering sker, såvida anstånd inte har beviljats av PTS. WhatsApp lämnade den kompletterade informationen till PTS den 18 november 2022, dvs. tre veckor från att den inledande informationen lämnades. PTS kan därmed konstatera att WhatsApp inte har rapporterat den inträffade säkerhetsincidenten inom de tidsramar som framgår av PTS säkerhetsföreskrifter.

För att efterleva kraven på uppgiftslämnande i 8 kap. 3 § LEK samt 17 kap. 1 – 5 §§ PTS säkerhetsföreskrifter ska WhatsApp inkomma med kompletterande information motsvarande samtliga uppgifter som ska rapporteras i en inledande och kompletterade rapport i enlighet med 17 kap. 3 och 4 §§ i PTS säkerhetsföreskrifter, såvida dessa uppgifter inte redan har rapporterats till PTS tidigare.

WhatsApp får tillfälle att yttra sig

PTS finner sammanfattningsvis att myndigheten enligt 11 kap. 5 § LEK ska underrätta WhatsApp om att myndigheten misstänker att WhatsApp agerar i strid med bestämmelserna om rapportering av säkerhetsincidenter i 8 kap. 3 § LEK samt 17 kap. 1 – 5 §§ PTS säkerhetsföreskrifter.

WhatsApp ges tillfälle att senast den 26 april 2023 yttra sig över denna underrättelse.

När tiden för att inkomma med yttrande har löpt ut kan PTS med stöd av 11 kap. 6 § LEK komma att meddela de förelägganden som behövs för att WhatsApp ska vidta nödvändiga åtgärder för rättelse. Eventuella förelägganden kan komma att förenas med vite. Om WhatsApp inte alls hörs av kan PTS ändå komma att fatta beslut på det underlag som står till myndighetens förfogande.

PTS kan också med stöd av 12 kap. 1 § 5 LEK besluta att ta ut en sanktionsavgift av den som inte rapporterar om säkerhetsincidenter i enlighet med 8 kap. 3 § LEK och PTS säkerhetsföreskrifter.

Ett beslut om underrättelse enligt 11 kap. 5 § LEK får enligt 15 kap. 4 § samma lag inte överklagas.

Underrättelsen har beslutats av enhetschef Johanna Eklund. Föredragande har varit Petra Nilsson. I ärendets slutliga handläggning har även Erika Hersaeus och verksjuristen Sofie Sandell deltagit.