Datum	Vår referens	Aktbilaga
2016-09-21	Dnr: 14-12990	42

Nätsäkerhetsavdelningen
[redacted]

Wexnet AB
[redacted]
c/o Växjö energi AB
Box 497
351 06 Växjö

Tillsyn om störningar och avbrott i elektroniska kommunikationsnät och -tjänster

Saken

Tillsyn med anledning av upprepade störningar och avbrott i allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster.

Post- och telestyrelsens avgörande

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

Bakgrund

Wexnet AB (Wexnet) drabbades av störningar och avbrott i sina elektroniska kommunikationsnät och -tjänster den 12 december 2013, den 4 februari 2014, den 21 mars 2014, den 16 oktober 2014, den 21 november 2014, den 26 november 2014 och den 30 december 2014. Störningarna och avbrotten varierade i tid mellan 4,5 timmar upp till 42,5 timmar.

Utifrån omfattningen och frekvensen av incidenterna beslutade PTS den 8 januari 2015 att inleda tillsyn över Wexnets driftsäkerhetsarbete. Inom ramen för tillsynen har PTS haft möte med Wexnet den 4 februari 2015 vid vilket Wexnet redogjorde för orsakerna till de inträffade incidenterna, vidtagna åtgärder för undvikande av liknande incidenter, eventuella förändringar av processer och rutiner som föranletts av de inträffade incidenterna samt hur fortsatt uppföljning kommer att ske för att åtgärda uppkomna fel. Vidare redogjorde Wexnet för sitt säkerhetsarbete och arbete med nätuppbyggnad, sina processer för riskhantering, incidenthantering och kontinuitetsplanering samt

för sitt förebyggande arbete i form av riskanalyser och säkerhetstester som genomförs innan driftsättning av nya tjänster och vid förändringsarbete.

Wexnet har sedan löpande sedan tillsynen inletts redogjort för status i det fortgående arbetet med såväl administrativa som tekniska åtgärder för att höja driftsäkerheten i sitt elektroniska kommunikationsnät.

Wexnet har bland annat lämnat in dokumentation i form av beskrivning av nätdesign, mall för incidentrapportering, mall för hantering av planerade och oplanerade driftsavbrott, checklista vid leverans, rutiner för förändringsarbete, dokument med krav för driftsättning, beredskapsinstruktion, delar av rapport avseende översyn av Wexnets nya nät, rutin för risk- och sårbarhetsanalys samt statistik över uppnådd tillgänglighet från och med januari 2016 till och med augusti 2016.

Utöver ovan redovisade störningar och avbrott har ytterligare incidenter drabbat Wexnet efter det att PTS beslutat att inleda tillsyn. Dessa har inträffat bland annat den 2 mars 2015, den 15 april 2015, den 3 augusti 2015 och den 21 november 2015 samt den 13 april 2016.

Inträffade incidenter och deras orsaker

Wexnet har sammanfattningsvis lämnat följande upplysningar.

Grundproblemet vid de först inträffade incidenterna i december 2013 och februari 2014 bestod i att Wexnet hade köpt in utrustning som hade en bristande kapacitet för nätdesignen, som därmed blev underdimensionerad. Omkring en fjärdedel av kunderna påverkades av detta problem. För att åtgärda problemen tillfälligt togs redundans bort i vissa delar av kommunikationsnätet för att underlätta trafikhanteringen, vilket innebar att kommunikationsnätet blev känsligare för störningar och avbrott. I maj/juni 2014 genomfördes förändringar i form av en interimslösning med core-switchar från en annan leverantör. Samtidigt bestämde Wexnet sig för att bygga ett nytt nät och använda sig av interimslösningen under tiden det tog att bygga upp och ta det nya nätet i drift.

Orsakerna till störningen den 12 december 2013 var ett hårdvarufel. Efter det att det felaktiga nätelementet bytts fungerade tjänsterna igen. Felet den 4 februari 2014 berodde på ett programvarufel i nätverksutrustningen. För att åtgärda problemen stoppades driftsättningen av det nya nätet i avvaktan på uppgradering av programvaran. Felen som inträffade i mars, oktober och

november 2014 berodde på s.k. arpstormar[1]. För att åtgärda dessa byggde företaget om delar av sitt kommunikationsnät och införde portisolation. Felet den 30 december 2014 berodde på ett hårdvarufel som åtgärdades genom att den felaktiga hårdvaran byttes ut.

Det nya nätet togs i drift i månadsskiftet november/december 2014 efter att man genomfört omfattande tester. Wexnet har använt sig av en annan leverantör och har även valt en ny integratör för genomförande av det fortsatta arbetet. De genomför flytten för några kunder i taget. Flytten inleddes det första kvartalet 2015 med en projekttid som beräknats löpa under 18 månader. Under en övergångsperiod kommer Wexnet således att ha två kommunikationsnät. Efter överflytt kommer samtliga kunder att hanteras i det nya nätet.

Orsakerna till incidenten den 2 mars 2015 var ett hårdvarufel då en server havererade. För att korrigera felet installerade de en ny och permanent server i Wexnets nya kommunikationsnät. Man har också infört redundans på denna server. Orsakerna till incidenten den 15 april 2015 berodde på en felkonfiguration i samband med överflyttning av tjänsteleverantörer från det gamla till det nya nätet. Incidenten den 3 augusti 2015 påverkade samtliga kunder men varade inte så länge att den var rapporteringspliktig till PTS. Incidenten berodde på felaktigheter i programvaran. Efter analys har korrigerande programvara installerats av deras leverantör. Incidenterna den 21 november 2015 respektive den 13 april 2016 berodde på ytterligare felaktigheter i programvaran. Tillfälliga konfigurationsändringar har införts för att kringgå effekterna av den felaktiga programvaran i avvaktan på installation av felkorrigerad programkod. Efter omfattande felsökning av programvaran under sommaren 2016 utan att finna den exakta felorsaken har de beslutat att byta ut den hårdvara som berörts av de senaste inträffade störningarna. Därefter kommer de att ha hårdvara från en och samma leverantör i sitt kommunikationsnät. Denna hårdvara kommer att vara renodlat avsedd för operatörsverksamhet. Detta kommer att innebära att kapaciteten i deras kommunikationsnät kommer att öka. Detta arbete kommer att påbörjas i september 2016 och beräknas pågå under 1,5 år.

Wexnet har även låtit ett konsultföretag genomföra en översyn och analys av hur det nya kommunikationsnätet fungerar samt lämna förslag på vilka åtgärder Wexnet bör vidta för att uppfylla de krav som följer av PTS föreskrifter och

[1] En s.k. Arpstorm kan förenklat beskrivas som Adresseringsproblem på lager två, MAC adresser försöker använda nätet och skickar trafik till den normala lager 2 switchen. Om adressen inte känns igen skickas trafiken vidare till nästa switch. Om inget svar uppstår där heller kan trafiken gå in i en loop med förfrågningar som skickas fram och tillbaka, vilket slutligen sänker trafiken.

allmänna råd om krav på driftsäkerhet (PTSFS 2015:2). När det gäller administrativa åtgärder har Wexnet utsett en informationssäkerhetsansvarig som organisatoriskt finns i Växjö energi AB och är placerad under VD. Vidare har man utökat internkontroller som ett led i sitt säkerhetsarbete. Detta arbete leds av den informationssäkerhetsansvarige. De har infört riskanalyser inför allt förändringsarbete som går utöver daglig drift. Vidare har de gått igenom och förtydligat sina instruktioner och processer som gäller för driften av kommunikationsnätet. De har förbättrat och dokumenterat sina processer för riskhantering, incidenthantering och kontinuitetsplanering.

Skäl

Tillämpliga bestämmelser

Av 5 kap. 6 b § lag (2003:389) om elektronisk kommunikation (LEK) framgår bl.a. att den som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet. De åtgärder som vidtas ska vara ägnade att skapa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för störningar och avbrott.

Bestämmelsen i 5 kap. 6 b § LEK förtydligas i PTS föreskrifter om krav på driftsäkerhet (PTSFS 2015:2), vilka trädde i kraft den 1 januari 2016.

Enligt 3 § i föreskrifterna ska tillhandahållarens driftsäkerhetsarbete bedrivas långsiktigt, kontinuerligt och systematiskt. Arbetet ska omfatta såväl normala driftsförhållanden som extraordinära händelser.

Tillhandahållaren ska i driftsäkerhetsarbetet ha en tydlig rollfördelning med särskilt utpekade ansvariga för arbetet. Vidare ska tillhandahållaren ta fram och dokumentera de processer, planer och tester som föreskrivs i 5, 7, 8, 12, 13, 21 och 22 §§ samt säkerställa att anställda och uppdragstagare har kunskap om de processer och planer som de är berörda av.

Enligt 5 § ska tillhandahållaren minst en gång per år analysera risken för att dokumenterade tillgångar och förbindelser enligt 4 § orsakar störningar eller avbrott i de kommunikationsnät och kommunikationstjänster som denne tillhandahåller.

Tillhandahållaren ska, utöver vad som föreskrivs i första stycket, genomföra riskanalyser inför sådana planerade förändringar som kan påverka driftsäkerheten i de kommunikationsnät och kommunikationstjänster som denne tillhandahåller, samt efter att sådana störningar eller avbrott som ska

rapporteras enligt 5 kap. 6 c § lagen (2003:389) om elektronisk kommunikation har inträffat.
Riskanalyserna enligt första och andra stycket ska innefatta åtminstone följande delar:
1. Identifiering av samtliga relevanta hot mot den aktuella tillgången eller förbindelsen. Hot relaterade till väder samt intrång och annan yttre påverkan ska alltid analyseras.
2. Kvalificerad bedömning av konsekvenser i händelse av att identifierade hot inträffar.
3. Kvalificerad bedömning av sannolikheten för att identifierade hot inträffar.
4. Kvalificerad sammanvägd bedömning av sannolikheten för att identifierade hot inträffar och de konsekvenser det kan medföra om de inträffar (riskbedömning).

Vid genomförande av riskanalyser ska tillhandahållaren beakta erfarenheter från inträffade incidenter samt tillämpa processer som utgår från etablerad standard på området.

Tillhandahållaren ska ha en plan för vid vilka tidpunkter och i vilka situationer tillhandahållaren kommer att genomföra riskanalyser.

Tillhandahållaren ska dokumentera genomförda riskanalyser.

Enligt 6 § ska tillhandahållaren analysera vilka konsekvenser som kan uppstå när kritiska verksamhetsdelar helt eller delvis upphör att fungera. Analysen ska omfatta en bedömning av när särskilda handlingsplaner enligt 8 § ska tillämpas. Konsekvensanalysen ska dokumenteras och revideras vid behov.

Enligt 7 § ska tillhandahållaren säkerställa att
1. inträffade incidenter rapporteras internt,
2. åtgärder vidtas skyndsamt för att hantera en uppkommen incident,
3. åtgärder vidtas för att undvika liknande incidenter, och
4. att erfarenheter från inträffade incidenter beaktas vid genomförande av riskanalyser enligt 5 §.
Vid vidtagande av åtgärder enligt första stycket (incidenthantering) ska tillhandahållaren tillämpa processer som utgår från etablerad standard på området.

Enligt 8 § ska Tillhandahållaren tillämpa särskilda handlingsplaner i enlighet med sin analys och bedömning enligt 6 §. Handlingsplanerna ska innefatta åtgärder för att begränsa de konsekvenser som kan uppstå enligt analysen samt för att återställa kritiska verksamhetsdelar till normal funktionsförmåga (kontinuitetsplanering).

Tillhandahållaren ska utgå från etablerad standard på området vid framtagande av handlingsplanerna. Tillhandahållaren ska revidera handlingsplanerna vid behov och öva planerna vartannat år.

Enligt 12 § ska Tillhandahållaren, innan denne genomför förändringar i sina kommunikationsnät och kommunikationstjänster som kan medföra störningar eller avbrott av betydande omfattning, säkerställa att tester utförs.

Tillhandahållaren ska planera för att återställa kommunikationsnätet och kommunikationstjänsten i händelse av att störning eller avbrott inträffar. Tester och planer för återställande ska vara anpassade till den planerade förändringens art och omfattning.

Tillhandahållaren ska tillämpa en process vid genomförande av planerade förändringar som utgår från etablerad standard på området.

PTS är enligt 2 § första stycket förordningen (2003:396) om elektronisk kommunikation tillsynsmyndighet enligt LEK. Tillsynsmyndigheten ska enligt 7 kap. 1 § LEK utöva tillsyn över bl.a. efterlevnaden av lagen samt de föreskrifter som har meddelats med stöd av lagen.

PTS bedömning

PTS kan inledningsvis konstatera att Wexnet drabbats av anmärkningsvärt många och omfattande störningar under den aktuella tidsperioden. Detta tyder bl.a. på att det förelegat brister i företagets långsiktiga, systematiska och kontinuerliga driftsäkerhetsarbete. PTS kan härvid konstatera att Wexnet under tillsynens gång i allt större utsträckning har prioriterat och fokuserat på driftsäkerhetsarbetet och löpande vidtagit åtgärder för att komma till rätta med problemen, vilket PTS ser positivt på. Myndigheten ser dock att driftsäkerhetsarbetet kontinuerligt behöver ses över och utvecklas och uppmanar därför Wexnet till att fortsätta arbetet med att tekniskt, organisatoriskt och processuellt säkerställa ett gott driftsäkerhetsarbete.

När det gäller de inträffade incidenterna och dess orsaker bedömer PTS att en delförklaring till incidenterna i december 2013 och början på 2014 är att Wexnet, mot bakgrund av brister i nätdesignen, tillfälligt tagit bort redundansen i vissa delar av kommunikationssystemet för att underlätta trafikhanteringen. Med fullgod redundans tas trafiken över av det redundanta systemet, t.ex. i samband med hårdvarufel. Ett fel behöver därför inte påverka slutkunderna annat än kortvarigt. I avsaknad av redundans kan dock även ett enstaka fel få en större påverkan, vilket var fallet för Wexnet. Mot bakgrund av ingiven

dokumentation och Wexnets redogörelse bedömer dock PTS att Wexnet uppfyller PTS krav på redundans för tillgångar i PTS föreskrifter om krav på driftsäkerhet.

De bakomliggande bristerna i nätdesignen bedömer PTS har sin förklaring i missförstånd eller otydligheter i samband med den kravställning som skett vid en tidigare genomförd upphandling, samt i brister i det förebyggande riskanalysarbetet vid förändringshantering. Det åligger Wexnet att säkerställa att de underleverantörer som företaget är beroende av kan uppfylla kraven på driftsäkerhet. En brist hos en underleverantör kan därför mycket väl innebära en brist i Wexnets driftsäkerhetsarbete. Inom ramen för tillsynen har Wexnet dock inlämnat godtagbar dokumentation avseende företagets kravspecifikation för upphandling av det nya nät som upphandlats, samt infört en rutin som säkerställer genomförande av riskanalyser i samband med förändringsarbeten som avviker från den dagliga driften. Man har även förbättrat sina instruktioner och rutiner som ska tillämpas i samband med förändringsarbetet samt infört en återställelseplan som tas fram inför alla större förändringar samt genomför tester. PTS bedömer att ovanstående åtgärder har minskat risken för incidenter hänförliga till brister i samband med upphandling och större förändringar, och lämnar med detta saken utan ytterligare åtgärd.

När det gäller de s.k. arpstormarna kan PTS konstatera att en första störning hänförlig till detta problem inträffade den 21 mars 2014. Därefter uppstod incidenter på grund av arpstormar på nytt den 16 oktober 2014, den 21 november 2014 och den 26 november 2014. Först i slutet av november 2014 vidtogs åtgärder i form av portisolation, vilket förefaller ha löst problemet. PTS kan konstatera att ytterligare incidenter på grund av arpstormar inte har rapporterats till myndigheten efter 2014, varför PTS i dagsläget inte vidtar någon ytterligare åtgärd i frågan. Det kan dock ifrågasättas om inte ytterligare utredningsresurser borde ha satts in i ett tidigare skede för att på ett snabbare sätt utreda felorsaken och hitta en lösning på problemet. PTS bedömer härvid att Wexnets rutiner för incidenthantering, inklusive företagets rutiner att vidta åtgärder för att liknande incidenter inte inträffar igen kan behöva ses över. Vidare är det av vikt att erfarenheterna från inträffade störningar beaktas vid genomförandet av förnyade riskanalyser. PTS förutsätter att Wexnet kommer att prioritera detta område i framtiden, vilket PTS kan komma att granska i kommande tillsynsinsatser.

Felen som inträffat i augusti och november 2015 och under våren 2016 har varit hänförliga till felaktigheter i programvaran. Dessa felaktigheter har åtgärdats genom uppgraderingar (patchning) av programvaran. Vissa kvarstående felaktigheter i programvaran har Wexnet beslutat att åtgärda genom utbyte av den hårdvara som är behäftad med felaktig programvara.

Investeringen i ny hårdvara görs dessutom för att uppnå enhetlighet och utökad kapacitet i kommunikationsnätet. PTS förutsätter att Wexnet genom ovannämnda åtgärder säkerställer att felen åtgärdas, och lämnar med detta påpekande även denna del av tillsynen utan ytterligare åtgärd.

Avslutningsvis vill PTS betona att säkerställande av en godtagbar driftsäkerhet är ett kontinuerligt arbete som behöver prioriteras löpande i Wexnets verksamhet. Det följer av PTS föreskrifter och är en grundförutsättning för att upprätthålla en rimlig nivå av driftsäkerhet som gäller för alla tillhandahållare av elektroniska kommunikationsnät- och tjänster som verkar i Sverige. Mot bakgrund av de åtgärder som Wexnet har vidtagit och med de påpekanden PTS har gjort ovan, kan myndigheten konstatera att det saknas anledning att i dagsläget vidta ytterligare åtgärder i ärendet, men myndigheten kan komma att återkomma till en granskning av Wexnets driftsäkerhetsarbete om fortsatta incidenter av de slag som här har varit föremål för granskning inträffar. Med detta konstaterande avskrivs ärendet från vidare handläggning.

Beslutet har fattats av enhetschefen Patrik Bystedt. I ärendets slutliga handläggning har även Björn Scharin och Peder Cristvall (föredragande) deltagit.