Avdelningen för säker kommunikation

Konsekvensutredning avseende föreskrifter om säkerhetsåtgärder för sektorn digital infrastruktur enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster

Post- och telestyrelsen (PTS) avser att med stöd av 8 § förordningen (2018:1125) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-förordningen) utfärda föreskrifter om säkerhetsåtgärder enligt 12-14 §§ lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster för sina tillsynsområden.

PTS redovisar härmed sin utredning enligt förordningen (2007:1244) om konsekvensutredning vid regelgivning.

Post- och telestyrelsen

Postadress:
Box 5398
102 49 Stockholm

Besöksadress:
Valhallavägen 117 A
www.pts.se

Telefon: 08-678 55 00
Telefax: 08-678 55 05
pts@pts.se

Innehåll

1 Inledning

Nätverks- och informationssystem, i synnerhet internet, spelar en viktig roll i samhället genom att underlätta den gränsöverskridande rörligheten för varor, tjänster och personer. På grund av denna transnationella natur kan allvarliga störningar av dessa system, vare sig de är avsiktliga eller oavsiktliga och oberoende av var de förekommer, påverka enskilda medlemsstater och unionen som helhet. Säkerheten i nätverks- och informationssystem är därför avgörande för att den inre marknaden ska fungera väl.

Europaparlamentet och rådet antog 2016 ett direktiv om åtgärder för en hög gemensam nivå på säkerhet i nätverk och informationssystem inom hela EU[1], det s.k. NIS-direktivet. Enligt NIS-direktivet ska företag som levererar samhällsviktiga och digitala tjänster inom EU följa samma krav på informationssäkerhet och incidentrapportering. NIS-direktivet genomfördes 2018 i Sverige genom en ny lag, lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen).

Syftet med NIS-lagen är att uppnå en hög nivå på säkerheten i nätverk och informationssystem för samhällsviktiga tjänster inom sju sektorer. NIS-lagen ställer bl.a. krav på att leverantörer av samhällsviktiga tjänster ska vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Åtgärderna ska säkerställa en nivå på säkerheten i nätverken och informationssystemen som är lämplig i förhållande till risken.

PTS är utsedd tillsynsmyndighet för sektorn digital infrastruktur och för leverantörer av digitala tjänster enligt 17-18 §§ i NIS-förordningen. Enligt 8 § i NIS-förordningen får PTS meddela föreskrifter om säkerhetsåtgärder enligt 12-14 §§ NIS-lagen för sektorn digital infrastruktur. Det finns sex ytterligare tillsynsmyndigheter: Transportstyrelsen, Finansinspektionen, Inspektionen för vård och omsorg, Livsmedelsverket och Statens Energimyndighet.

Syftet med de nu föreslagna föreskrifterna är att säkerställa en hög säkerhetsnivå för nätverk och informationssystem som används för att tillhandahålla den samhällsviktiga tjänsten inom sektorn digital infrastruktur samt förtydliga vad skyldigheterna om säkerhetsåtgärder innebär i NIS-lagen för sektorn digital infrastruktur.

Med ”nätverk och informationssystem” avses i den fortsatta framställningen sådana nätverk och informationssystem som används för att tillhandahålla den samhällsviktiga tjänsten inom digital infrastruktur.

[1] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen

Föreskrifter meddelade av Myndigheten för samhällsskydd och beredskap

Myndigheten för samhällsskydd och beredskap (MSB) har en sammanhållande roll för NIS-regleringen och berörda tillsynsmyndigheter, exempelvis när det gäller tillsyn och framtagande av föreskrifter. MSB har utfärdat förskrifter och allmänna råd för:

- anmälan och identifiering av leverantörer av samhällsviktiga tjänster[2] (MSB:s anmälningsföreskrifter),
- informationssäkerhet för leverantörer av samhällsviktiga tjänster[3] (MSB:s informationssäkerhetsföreskrifter),
- rapportering av incidenter för leverantörer av samhällsviktiga och digitala tjänster (MSB:s incidentrapporteringsföreskrifter)[4],
- om rapportering av incidenter för leverantörer av digitala tjänster[5] samt
- frivillig incidentrapportering för tjänster som är viktiga för samhällets funktionalitet[6].

Av MSB:s anmälningsföreskrifter framgår att de nätverk och informationssystem som regleras i direktivet och som faller inom PTS verksamhetsområden när det gäller samhällsviktiga tjänster inom sektorn digital infrastruktur är de nätverk och informationssystem som används för att tillhandahålla följande tjänster:

- Registreringsenheter för toppdomäner (även kallade toppdomänadministratörer eller TLD name registries) (för mer information se avsnitt 2.1) och
- DNS-tjänster i form av auktoritativ och rekursiv namnservertjänst (för mer information se avsnitt 2.1).

Sambandet mellan MSB:s informationssäkerhetsföreskrifter och PTS nu föreslagna föreskrifter om säkerhetsåtgärder

MSB har meddelat föreskrifter om det systematiska och riskbaserade informationssäkerhetsarbetet som leverantörer av samhällsviktiga tjänster ska bedriva enligt 11 § lagen NIS-lagen (MSB:s informationssäkerhetsföreskrifter). Dessa föreskrifter omfattar bl.a. övergripande krav på genomförande av riskanalyser, införande av ändamålsenliga och proportionella säkerhetsåtgärder, interna regler och arbetssätt för att tillse att medarbetarna har kunskap om säker hantering av information och kontinuitetsplanering. Även de nu föreslagna

---

[2] Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster, MSBFS 2018:7
[3] Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster, MSBFS 2018:8
[4] Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster, MSBFS 2018:9
[5] Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd om rapportering av incidenter för leverantörer av digitala tjänster, MSBF 2018:10
[6] Myndigheten för samhällsskydd och beredskaps föreskrifter om frivillig rapportering av incidenter i tjänster som är viktiga för samhällets funktionalitet, MSBFS 2018:11

föreskrifterna från PTS uppställer bl.a. krav på riskanalyser, att införa proportionella säkerhetsåtgärder, att säkerställa medarbetares kompetens och krav på kontinuitetsplanering. Leverantörer av samhällsviktiga tjänster omfattas således redan av liknande krav som nu föreslås. PTS nu föreslagna föreskrifter förtydligar MSB:s säkerhetsföreskrifter och är sektorspecifika.

I sammanhanget är det även värt att notera att det är tillsynsmyndigheterna som har rätt att utöva tillsyn över MSB:s föreskrifter inom NIS-området. Det vill säga PTS utövar tillsyn inte bara över NIS-lagen och myndighetens egna föreskrifter utan också över MSB:s föreskrifter inom sektorn digital infrastruktur.

2 Beskrivning av problemet och vad PTS vill uppnå

Säkerhetsincidenter, som blir allt mer omfattande och vanliga och får allt större inverkan, utgör ett allvarligt hot mot nätverks- och informationssystemens funktion. Dessa system kan också bli mål för avsiktligt sabotage i syfte att skada dem eller förorsaka driftsavbrott. Sådana incidenter kan hindra genomförandet av ekonomisk verksamhet, generera omfattande ekonomiska förluster, undergräva användarnas förtroende och medföra allvarliga konsekvenser för Sveriges ekonomi.

2.1 Domännamnssystemet – väsentligt för fungerande digitalt samhälle

Det globala domännamnssystemet, Domain Name System förkortat DNS, är den bakomliggande tekniska infrastruktur som genomför domännamnsuppslagningar på internet åt internetanvändare och applikationer. DNS anses som en av de viktigaste funktionerna för att internet ska kunna fungera praktiskt för internetanvändare. Om DNS blir otillgängligt, går det inte att göra domännamnuppslagningar och då upplevs internet som förhållandevis obrukbart för användarna, eftersom det varken går att exempelvis surfa eller skicka e-post då.

DNS är ett hierarkiskt, decentraliserat och distribuerat uppbyggt namnsystem för genomförande av domännamnsuppslagningar på internet. Det är uppbyggt i minst tre nivåer för att hantera den globala DNS-lastbalanseringen. Dessa nivåer är rotnivå eller roten, toppdomännivå, huvuddomännivå.

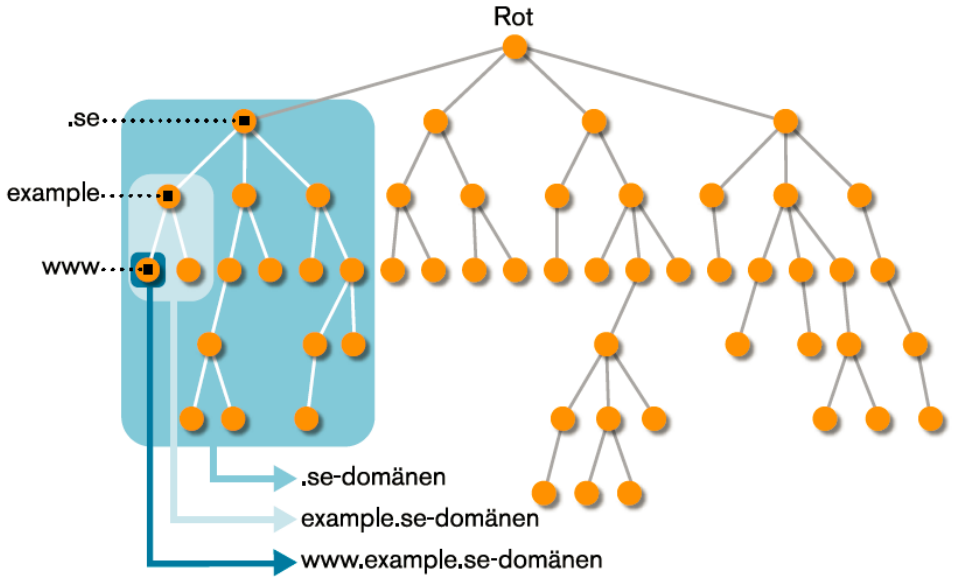
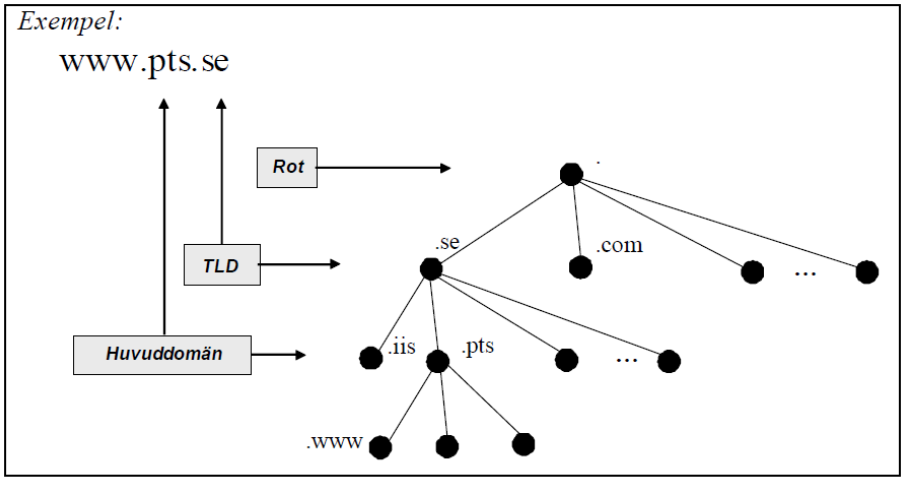


Bild Internetstiftelsens rapport DNS – Internets vägvisare, https://www.iis.se/fakta/dns-internets-vagvisare/

Den s.k. roten (även kallad rotservern eller rotnamnservertjänsten) finns på den översta nivån i DNS-systemhierarkin och innehåller information om ip-adresserna till toppdomänernas s.k. auktoritativa namnservrar. Internet Corporation for Assigned Names and Numbers, ICANN, ansvarar för den tekniska samordningen av DNS och för vilka toppdomäner som finns på internet. I praktiken sker det via IANA-funktionen[7] som ansvarar för teknisk drift av den s.k. primära auktoritativa namnservertjänsten för roten.

Idag finns det ca 1100 *auktoritativa rotnamnservrar*[8] utspridda över världen. Dessa sköts av tolv oberoende rotnamnserveroperatörer. En av dessa rotnamnserveroperatörer finns i Sverige och ansvarar för elva instanser (kopior) av roten. Det stora antalet auktoritativa namnservrar på rotnivå utspridda över världen gör att de tillsammans skapar en robust och redundant DNS-infrastruktur. Rotnamnservrarna behöver i praktiken inte innehålla så mycket information eftersom ett stort ansvar för DNS-informationen har delegerats ned till nästa nivå i hierarkin, toppdomänerna.

Toppdomänerna (t.ex. .se, .fi, .dk, .fr, .com, .org) pekar ut adresserna till de s.k. auktoritativa namnservrarna för huvuddomänerna. Registreringsenheter för toppdomäner (även kallade toppdomänadministratörer) ansvarar för den tekniska driften av toppdomännamnservertjänst och för förvaltning av domännamnsregister över tilldelade domännamn under respektive toppdomän.



På nästa nivå längre ner i hierarkin finns namnservrarna för de s.k. huvuddomänerna, t.ex. pts.se. En huvuddomän ansvarar för att finna ip-adressen till webbservern för det domännamn som internetanvändaren har eftersökt.

[7] Internet Assigned Numbers Authority

[8] http://www.root-servers.org/

Att DNS är hierarkiskt och distribuerat medför att ansvaret för DNS är delat på flera aktörer, där var och en har ansvar för DNS-informationen för sin del av trädstrukturen (även kallad zon). Det för med sig att domänerna längre ned i hierarkin är beroende av att de högre nivåerna fungerar, så att delegeringen verkligen sker och det går att hitta fram till den IP-adress som är knuten till ett visst domännamn. Däremot är de högre nivåerna i hierarkin inte beroende av sina underdomäner. Denna ansvarsfördelning gör infrastrukturen mindre känslig, men ansvaret är större i de övre nivåerna i systemet.

Den som vill registrera ett domännamn på internet, t.ex. pts.se, måste vända sig till en återförsäljare av domännamn (även kallad registrar). I samband med registrering av ett domännamn måste sedan minst *en auktoritativ namnserver* pekas ut för domännamnet, annars går det inte att hitta fram till domänen via DNS. Det kan antingen vara en namnserver som innehavaren av domännamnet själv gör tillgänglig på internet eller också en namnserver som drivs av någon annan, t.ex. en internetleverantör eller ett s.k. webbhotell.

Slutligen, för att slutanvändaren ska kunna nyttja den information som DNS tillhandahåller behövs också en programvara som ställer frågan ”vilken IP-adress ett domännamn motsvarar”. Detta sker dels av en programvara som finns i användarens dator, en s.k. stub resolver, dels av en rekursiv namnserver som vanligtvis finns hos internetleverantören. För att hindra DNS-uppslagningar från att ta för lång tid och orsaka onödigt mycket nätverkstrafik, kan en rekursiv namnserver tillfälligt lagra svar som den får från auktoritativa namnservrar i sitt cacheminne. När en fråga kommer till den rekursiva namnservern kontrollerar den först om det finns några uppgifter i cacheminnet som kan hjälpa till för att svara på den. Hur länge svaren lagras av den rekursiva namnservern bestäms av ett värde som anges av den som är ansvarig för zonen, en s.k. TTL (time to live). När denna tidsperiod är slut sparas uppgiften inte längre, då måste den rekursiva namnservern kontakta någon av zonens auktoritativa namnservrar nästa gång en domännamnsuppslagning görs.

Transporten av DNS-informationen sker genom ett antal internetleverantörer som måste tillhandahålla fungerande nätverk med tillräcklig kapacitet.

2.2 Omvärldsbild och närmare om problemen

En av de vanligaste orsakerna till incidenter som påverkar DNS-tjänsten är den mänskliga faktorn, t.ex. av misstag felkonfigurerade namnservrar. En annan orsak till incidenter är olika former av logiska attacker. Dessa attacker kan bestå i att DNS-information manipuleras, dvs. att informationens riktighet och äkthet (autenticitet) inte kan bevaras eller genom onormalt hög belastning på DNS, som orsakas av att frågeställare ställer upprepade frågor i stor mängd i illvilligt syfte. Falsk DNS-information medför risk för att trafik leds till en icke-efterfrågad webbplats, information stjäls eller att transaktioner störs. En överbelastningsattack kan leda till att en DNS-tjänst inte kan upprätthållas, vilket kan leda till att internetanvändaren upplever ett avbrott.

Av aktuell omvärldsbevakning framgår att DNS-infrastrukturen, på olika nivåer, i allt högre utsträckning utsätts för riktade attacker och att överbelastningsattackerna ökar i storlek år för år. Om en attack mot en DNS-leverantör lyckas, kan den få stora konsekvenser för ett stort antal olika typer av webbtjänster och verksamheter påverkas t.ex. genom att bli eller upplevas vara otillgängliga. Nedan följer några exempel på attacker och hot:

- Vid årsskiftet 2018/2019 skedde en logisk attack mot DNS, när en s.k. Man-in-the-Middle-attack[9] drabbade flera DNS-leverantörer i flera länder och världsdelar. Även en svensk leverantör av samhällsviktiga tjänster inom sektorn digital infrastruktur drabbades av denna.

- En annan förhållandevis nyligen utförd attack mot DNS med stora konsekvenser, den största överbelastningsattacken hittills, genomfördes mot en stor och global DNS-leverantör i slutet av 2016. Denna medförde stora konsekvenser för bl.a. stora onlineåterförsäljare, medieföretag, spelplattformar och digitala betalningstjänster (e-payment services), som upplevde allvarliga störningar och avbrott.

- Ett ytterligare exempel är överbelastningsattacken som riktades mot internets rotnamnservrar under november och december 2015, då tre av internets tretton ursprungliga rotnamnservertjänster slogs ut under flera timmar, trots användning av anycastadressering[10]. ”Den svenska roten”, I-rotnamnservertjänsten, blev inte otillgänglig under denna attack.

- Vid svag säkerhetskontroll för åtkomst till domännamnsadministration finns risk för att obehörig uppdatering av DNS-uppgifter i den primära namnservern inträffar. När det gäller åtkomstkontroll till DNS-uppgifter krävs därför avancerade funktioner för kontroll av identitet och behörighet. En svensk leverantör av samhällsviktig tjänst inom sektorn digital infrastruktur drabbades 2017 av ett logiskt intrång till ett av bolagets informationssystem innehållande bl.a. kundernas autentiseringsuppgifter.

- En dåligt skyddad rekursiv namnserver som lagrar DNS-information i cache (dvs. sparar tidigare inhämtad information under en viss tid för att slippa fråga på nytt alltför ofta), kan få den cachade informationen obehörigen förändrad (s.k. cache poisoning). Detta kan leda till att den rekursiva namnservern levererar en felaktig IP-adress till frågeställaren under hela giltighetstiden som kan vara flera dagar (dvs. tills dess att tiden har gått ut för sparad adressinformation). Giltighetstiden styrs av

[9] där en antagonist kan läsa, tillföra och ändra meddelanden som skickas mellan två parter utan att någondera parten vet om att länken mellan dem har blivit komprometterad

[10] Med anycastadressering kan flera identiska namnservrar tilldelas samma IP-adress som då kan dela på arbetet med att besvara DNS-frågor.

TTL-parametern (Time To Live). Resultatet kan bli att trots att korrekt webbadress angivits i webbläsarens adressfält, hamnar användaren på helt fel webbserver, vilket skapar stor förvirring hos såväl användaren som hos innehavaren av den eftersökta webbsidan. Den rekursiva namnservern måste därför vara skyddad mot intrång och andra angrepp.

- En internetanvändare som tror sig vara ansluten till en viss rekursiv namnserver, kan också bli lurad genom s.k. adress spoofing så att en annan dator än den avsedda utger sig för att vara en rekursiv namnserver. Resultatet blir liknande det vid cache poisoning.

Antalet attacker mot DNS förutspås fördubblas från 2018 till 2023. Att överbelastningsattackerna förväntas öka kommer att kräva vidareutvecklade säkerhetsåtgärder.

2.3 Behov av föreskrifter om säkerhetsåtgärder

Problemen som redovisas ovan behöver motverkas och om de ändå inträffar behöver konsekvenserna av dem mildras. De nu föreslagna föreskrifterna syftar till att förtydliga vad skyldigheterna om säkerhetsåtgärder enligt 12-14 §§ NIS-lagen innebär och därigenom uppnå en hög nivå på säkerhet i nätverk och informationssystem för samhällsviktiga tjänster inom sektorn digital infrastruktur. Med de föreslagna kraven på säkerhetsåtgärder ska det bli lättare för leverantörerna att veta vilka skyldigheter om säkerhetsåtgärder som de behöver efterfölja.

2.4 Alternativa lösningar och effekter om föreskrifter inte tas fram

PTS har utvärderat följande alternativ till föreslagna föreskrifter:

- att inte ta fram föreskrifter,
- att avvakta med att ta fram föreskrifter,
- att i föreskrifterna ställa ett flertal tekniskt detaljerade krav på *hur* leverantörer ska ”uppnå ett visst skydd” med angivna krav på säkerhetsåtgärder från PTS oaktat vad leverantörens riskanalys visar samt
- att i föreskrifterna ställa formkrav på riskanalys, åtgärdsplan och ”*vad*-krav” på säkerhetsåtgärder sett till resultatet av leverantörens genomförda riskanalys (riskbedömningen), samt åtgärder avseende kontinuitetsplanering.

2.4.1 Att inte ta fram eller att avvakta med att ta fram föreskrifter

Ett alternativ är att inga föreskrifter tas fram. NIS-lagen ställer krav på att leverantörerna av samhällsviktiga tjänster vidtar ändamålsenliga och proportionella tekniska och organisatoriska åtgärder i förhållande till risken samt lämpliga åtgärder för att förebygga och minimera verkningar av incidenter (12 -14 §§).

Ett annat alternativ skulle kunna vara att avvakta med att ta fram föreskrifter för att istället bedriva tillsyn över de aktuella bestämmelserna i NIS-lagen (11-14 §§) och MSB:s informationssäkerhetsföreskrifter i syfte att få mer information om marknaden innan myndigheten beslutar att ta fram föreskrifter.

Alternativen att inte ta fram föreskrifter eller avvakta med att ta fram föreskrifter kan innebära att leverantörerna kommer att tolka kraven i lagen på olika sätt, vilket kan leda till ökad sårbarhet hos vissa leverantörer som väljer att vidta säkerhetsåtgärder i alltför liten utsträckning. Den regulatoriska osäkerheten kan därmed ge upphov till en oönskad konkurrensmässig obalans mellan leverantörerna. I förlängningen skulle också otydliga regler kunna leda till en viss förhöjd risk för incidenter i nätverk och informationssystem som tillhandahålls av de leverantörer som inte vidtar tillräckliga säkerhetsåtgärder.

I det fall några föreskrifter om säkerhetsåtgärder enligt 12-14 §§ NIS-lagen inte tas fram kan det dessutom ifrågasättas om Sverige kan anses ha införlivat NIS-direktivet eftersom medlemsstater ska ha vidtagit alla nödvändiga åtgärder för att se till att tillämpa regler om sanktioner[11].

PTS gör därmed bedömningen att föreskrifter behöver tas fram.

2.4.2 Detaljerade krav på säkerhetsåtgärder oaktat leverantörens riskanalys

Ett alternativ skulle kunna vara att ta fram preciserade krav på vilka säkerhetsåtgärder som samtliga leverantörer ska vidta oaktat vad leverantörernas riskanalyser visar. Ett sådant alternativ säkerställer en hög gemensam nivå på tillförlitlighet och säkerhet. I det fallet skulle emellertid leverantörens riskanalys spela en mindre roll vid valet av säkerhetsåtgärder än vad avsikten med lagstiftningen tycks vara. Lagstiftningen utgår från att det är en leverantörs riskanalys som ska ligga till grund för val av säkerhetsåtgärder. Dessutom kan en alltför detaljerad reglering bli inaktuell och riskera att hindra teknisk utveckling och konkurrens.

PTS gör därför bedömningen att alternativet inte är aktuellt i nuläget.

2.4.3 Säkerhetsåtgärder som leverantören vidtar utifrån sin riskanalys är det lämpligaste regeringsalternativet

Föreskrifter om säkerhetsåtgärder som innebär att leverantören ska genomföra säkerhetsåtgärder i de fall leverantörens riskanalys påvisar brister, leder till en tydligare reglering. Detta skapar regulatorisk förutsägbarhet, vilket i sin tur motverkar osäkerhet hos leverantörerna om vad som krävs av dem. Ur ett tillsynsperspektiv och för att kunna utfärda sanktioner, är det lämpligt och önskvärt för både leverantörer och tillsynsmyndigheter med krav på riskanalys, säkerhetsåtgärder som behöver vidtas i de fall leverantörens riskanalys utvisar brister samt kontinuitetsplanering. Föreskrifter om säkerhetsåtgärder

[11] Art.21 NIS-direktivet

säkerställer därmed i högre grad en hög gemensam nivå på tillförlitlighet och säkerhet i nätverk och informationssystem.

Alternativet som innebär att PTS först och främst reglerar genomförande av riskanalys, bedömningsgrunder för riskanalys och riskbedömning, åtgärdsplan, säkerhetsåtgärder och åtgärder för att förebygga och minimera verkningar av incidenter (kontinuitetsplanering) tillgodoser både kravet på en hög gemensam nivå på tillförlitlighet och säkerhet och möjligheten för leverantörerna att lägga sin riskanalys till grund för valet av säkerhetsåtgärder, såsom föreskrivs i 12 § NIS-lagen. Det här alternativet bidrar till regulatorisk förutsägbarhet genom att myndigheten i föreskrifterna tydliggör hur en riskanalys ska göras och vad den ska omfatta samt vad som behöver åtgärdas om leverantören i sin riskbedömning kommer fram till att vissa risker behöver åtgärdas.

PTS gör sammantaget bedömningen att föreskrifter om säkerhetsåtgärder ska tas fram och tydliggöra *vad* leverantörerna behöver analysera för att hantera risker som hotar säkerheten i nätverk och informationssystem, men samtidigt möjliggöra för leverantörerna att välja *hur* de ska åtgärda identifierade risker.

3 Aktörer som berörs av regleringen

3.1 Berörd bransch och kategori av företag

MSB:s anmälningsföreskrifter identifierar vilka typer av DNS-leverantörer som omfattas, nämligen leverantörer av *s.k. auktoritativa* och *s.k. rekursiva namnservertjänster, samt registreringsenheter för toppdomäner*. Anmälningsföreskrifterna definierar även ”tröskelvärden” för när en leverantör anses vara en leverantör av en samhällsviktig tjänst inom digital infrastruktur.

Sektorn digital infrastruktur utgörs av leverantörer som tillhandahåller samhällsviktiga tjänster på samtliga tre nivåer i domännamnssystemet (rotnivå, toppdomännivå och huvuddomännivå), och därmed tillhandahåller olika tjänster vid domännamnuppslagning på internet. Dessutom finns det en leverantör av rekursiv namnservertjänst i sektorn. Leverantörer av rekursiva och auktoritativa namnservertjänster tillhandahåller olika typer av namnservertjänster. Att vara en leverantör av en auktoritativ namnservertjänst innebär en större och mer komplex DNS-verksamhet än för en leverantör av rekursiv namnservertjänst. Leverantörer av auktoritativa namnservertjänster ansvarar för fler nätverk och informationssystem när det gäller tillhandahållande av den samhällsviktiga tjänsten än leverantörer av rekursiv namnservertjänst.

Aktörerna på en viss nivå i DNS-trädet, exempelvis leverantörer av auktoritativ namnservertjänst på huvuddomännivå, erbjuder vanligen liknande tjänster såsom registrering av domännamn, webb-, DNS-, e-post-hosting (dvs. att aktörerna erbjuder teknisk drift av webb-, DNS- och e-posttjänster mot ersättning). Mot bakgrund av att marknaden för ovanstående tjänster visar tendenser på att vara mättad, med en avstannande mängd av nyregistreringar av domännamn, börjar flera aktörer erbjuda nya typer av tjänster såsom molntjänster och drift av applikationer.

Vidare kännetecknas marknaden för auktoritativa namnservertjänster, såväl på toppdomännivå som huvuddomännivå, för närvarande av konsolidering mot bakgrund av minskad tillväxt avseende antalet nyregistreringar.

En rekursiv namnservertjänst tillhandahålls allt som oftast som en del av en internetanslutningstjänst, dvs. av internetoperatörer. Det finns bolag som tillhandahåller s.k. publika rekursiva namnservertjänster fristående från en internetanslutningstjänst. Exempel på sådana företag är Google[12], Oracle[13], IBM

[12] Rekursiv namnservertjänst Google Public DNS, https://developers.google.com/speed/public-dns
[13] Rekursiv namnservertjänst DynDNS, https://dyn.com/dns/

och Packet Clearing House och Global Cyber Alliance[14], Cisco[15], Cloudflare och APNIC[16] samt Amazon[17].

3.2 Antalet företag som berörs och storleken på företagen

Det finns förhållandevis få leverantörer av samhällsviktiga tjänster inom sektorn digital infrastruktur. Antalet anmälda leverantörer av samhällsviktiga tjänster inom sektorn digital infrastruktur med nu gällande anmälningsföreskrifter[18] från MSB uppgår till knappt ett dussin. NIS-regleringen är fortfarande förhållandevis ny och fler leverantörer av samhällsviktiga tjänster inom sektorn digital infrastruktur kan komma att anmäla sig, t.ex. i takt med tillväxten hos DNS-leverantörer eller på grund av reviderade tröskelnivåer i anmälningsföreskrifterna.

Med nu gällande regler finns det *en* registreringsenhet för toppdomäner som levererar samhällsviktiga tjänster enligt NIS-regleringen[19] i Sverige. Denna ansvarar för *två* samhällsviktiga tjänster:

- toppdomännamnservertjänst för den svenska nationella toppdomänen .se samt
- toppdomännamnservertjänst för den nationella toppdomänen .nu.

Registreringsenheten för den svenska nationella toppdomänen .se och för den nationella toppdomänen .nu, Internetstiftelsen, ansvarar för drygt 1 500 000 domännamn under toppdomänen .se samt för ca 260 000 domännamn under toppdomänen .nu.

PTS kan konstatera att leverantörerna av samhällsviktiga tjänster inom sektorn digital infrastruktur är av varierande storlek och kan sägas erbjuda DNS-tjänster på olika marknader. Det är skillnad, som tidigare beskrivits, på att vara en leverantör av samhällsviktig tjänst på rotnivå, toppdomännivå och huvuddomännivå samt på att tillhandahålla en rekursiv namnservertjänst. Vidare, när det gäller leverantörerna av auktoritativa namnservertjänster, är det en stor skillnad på de leverantörer som precis når upp till kravet (tröskelvärdet) i MSB:s anmälningsföreskrifter och på de som ansvarar för en DNS-tjänst med fler än en miljon registrerade och aktiva domännamn.

För de anmälda leverantörerna, som är svenska aktiebolag, finns uppgifter om bolagens årsomsättning och antalet anställda. Antalet anställda hos dessa

[14] Rekursiv namnservertjänst Quad9 Domain Name System Service, https://www.quad9.net/
[15] Rekursiv namnservertjänst OpenDNS, https://www.opendns.com/
[16] Rekursiv namnservertjänst 1.1.1.1, https://1.1.1.1/dns/ och https://www.cloudflare.com/learning/dns/what-is-1.1.1.1/
[17] DNS-tjänster Route 53, https://aws.amazon.com/route53/
[18] MSBFS 2018:7 föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster, https://www.msb.se/externdata/rs/0264c176-6b31-43c6-9fd8-807102df3844.pdf
[19] MSBFS 2018:7 föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster, https://www.msb.se/externdata/rs/0264c176-6b31-43c6-9fd8-807102df3844.pdf

varierar mellan en och 65 personer. I snitt har dessa leverantörer 27,11 anställda och medianen är 27 anställda. Omsättningen varierade mellan knappt 26 miljoner till ca 182 miljoner kronor med ett medelvärde om 68,36 och ett medianvärde om 34,03 miljoner kronor. Därtill finns också två svenska stiftelser, vilka har cirka 30 respektive 70 anställda, men vars årsomsättning är okänd. Vidare finns en aktör, som är ett av världens största bolag, vilken är etablerad som filial i Sverige och har anmält att de tillhandahåller både en auktoritativ och en rekursiv namnservertjänst.

4 Föreslagna krav och dess konsekvenser

4.1 Kostnadsmässiga och andra konsekvenser av föreslagna krav och allmänna råd

4.1.1 Allmänt

De föreslagna föreskrifterna innehåller bestämmelser om tekniska och organisatoriska säkerhetsåtgärder för leverantörer av samhällsviktiga tjänster inom sektorn digital infrastruktur. Föreskrifterna reglerar i huvudsak genomförande av riskanalys inklusive riskbedömning, framtagande av åtgärdsplan, säkerhetsåtgärder beroende på utfallet av leverantörens genomförda riskanalys samt åtgärder kopplade till kontinuitetsplanering.

4.1.2 Kostnadsuppskattningar

I följande avsnitt beskrivs föreslagna föreskrifter och allmänna råd samt PTS bedömning av de ekonomiska konsekvenserna för berörda leverantörer.

Berörda leverantörers kärnverksamhet består bl.a. av att tillhandahålla den nu utpekade samhällsviktiga tjänsten. Det innebär att leverantörerna, vad PTS förstår, redan har en robust teknisk infrastruktur samt vidtar säkerhetsåtgärder löpande för de nätverk och informationssystem som används för att tillhandahålla den samhällsviktiga tjänsten.

De nu föreslagna bestämmelserna från PTS förtydligar befintliga krav i MSB:s informationssäkerhetsföreskrifter (för mer information, se kapitel 1). I ljuset av att leverantörerna redan har teknisk infrastruktur och processer för att kunna tillhandahålla en fungerande samhällsviktig tjänst inom sektorn digital infrastruktur samt att krav i NIS-lagen och MSB:s informationssäkerhetsföreskrifter har funnits sedan 2018 förutsätter PTS att leverantörerna till största delen har de rutiner och processer samt den dokumentation som framgår av MSB:s informationssäkerhetsföreskrifter och som nu föreslås i PTS föreskrifter.

De kostnader som beräknas är en uppskattning av de tillkommande kostnader som leverantörerna skulle kunna få genom PTS nu föreslagna föreskrifter exempelvis om leverantören inte har genomfört en riskanalys, vidtagit säkerhetsåtgärder vid konstaterade tekniska eller organisatoriska brister i säkerheten, eller inte utfört kontinuitetsplanering för nätverk och informationssystem i den utsträckning som PTS reglerar.

Det är elva företag av varierande storlek som berörs (för mer information, se kapitel 3). Föreslagna föreskrifter kan sammanfattas medföra i första hand att företagen ska se till att processer och rutiner vid behov kompletteras och tillämpas samt att dokumentation vid behov kompletteras och hålls uppdaterad. Även om företagen är av varierande storlek och sannolikt har olika många nätverk och informationssystem, bedömer PTS att framför allt antalet informationssystem som används för att tillhandahålla den samhällsviktiga

tjänsten inte skiljer sig åt i någon betydande omfattning mellan leverantörerna. Vidare möjliggör föreskrifterna att leverantörerna kan gruppera liknande nätverk och informationssystem och på annat sätt effektivisera framtagandet av processer, rutiner och dokumentation. Med andra ord skulle det kunna betyda att oavsett antalet nätverk och informationssystem behöver lika antal processer, rutiner samt dokumentation tas fram. PTS bedömer därmed inte att föreslagna regler medför olika kostnader för leverantörerna av samhällsviktig tjänst inom sektorn digital infrastruktur.

Kostnaderna för potentiella ändringar redovisas som administrativa engångskostnader, administrativa årliga kostnader samt som övriga kostnader. PTS redovisar kostnader genom att ange uppskattat antalet timmar som krävs för att exempelvis initialt komplettera processer samt årligen för exempelvis revidering. Den initiala samt årliga tidsåtgången har sedan multiplicerats med timkostnaden för att få fram den totala administrativa kostnaden. Nivån på timkostnaden baseras på statistik från SCB. De aktuella kostnaderna baseras på driftingenjörer (telekommunikation) med civilingenjörsutbildning (SSYK-kod 2143). Inom den privata sektorn uppgår medellönen till 46 000 kronor i månaden i 2018-års löner. I beräkningarna antas alla arbeta 165 timmer per månad. I beräkningen av timkostnaden för företagens egen personal inkluderas semestertillägg (12 procent av en månadslön på årsbasis) samt 31,42 procent arbetsgivaravgift. Därefter har en 25-procentig overheadkostnad lagts på. Detta ger följande: 46 000/165 = 279 kronor 279* (0,12+0,3142) = 121 121+279 = 400 kronor per timme * 1,25 = 500 kronor per timme. PTS har således valt att räkna med kostnaden 500 kr/timme.

I de fall kostnaderna är helt avhängigt resultatet av leverantörens riskanalys har PTS valt att exemplifiera åtgärder som kan ge upphov till kostnader.

4.2 Tillämpningsområde samt ord och uttryck 1-3 §§

1 § Dessa föreskrifter innehåller bestämmelser om säkerhetsåtgärder för nätverk och informationssystem som används för att tillhandahålla samhällsviktiga tjänster inom sektorn digital infrastruktur enligt 12-14 §§ lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

2 § Uttryck som används i dessa föreskrifter har samma innebörd som i lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

3 § I dessa föreskrifter avses med

DNS: domännamnssystemet (Domain Name System),

nätverk och informationssystem: sådana nätverk och informationssystem som används för att tillhandahålla den samhällsviktiga tjänsten inom digital infrastruktur.

I 1 § klargörs tillämpningsområdet för föreskrifterna. För att tydliggöra innehållet i den föreslagna regleringen återfinns i 2-3 §§ en förklaring av begrepp som används i föreskrifterna.

PTS bedömer att 1 - 3 §§ inte medför några konsekvenser.

4.3 Riskanalys, riskbedömning och dokumentation 4 – 5 §§

Genomförandet av riskanalyser är en förutsättning för ett systematiskt och riskbaserat säkerhetsarbete eftersom det innebär att klargöra och analysera samt hantera de risker som hotar nätverk och informationssystem som används för att tillhandahålla den samhällsviktiga tjänsten. För att en leverantör ska kunna identifiera vilka åtgärder som är relevanta att vidta för att hantera riskerna är det nödvändigt att leverantören genomför en riskanalys[20].

4 § Leverantören ska identifiera samtliga nätverk och informationssystem.

Leverantören ska därefter genomföra riskanalyser för de nätverk och informationssystem som har identifierats.

En riskanalys ska åtminstone innefatta följande delar:

1. identifiering av samtliga relevanta hot mot nätverk och informationssystem,

2. en kvalificerad bedömning av vilka konsekvenser det får för säkerheten i nätverk och informationssystem i händelse av att hot mot nätverk och informationssystem inträffar,

3. en kvalificerad bedömning av sannolikheten för att hot mot nätverk och informationssystem inträffar,

4. en riskbedömning bestående av en kvalificerad sammanvägd bedömning av sannolikheten för att hot mot nätverk och informationssystem inträffar och de konsekvenser det kan medföra om de inträffar och

5. en bedömning om riskerna ska elimineras, reduceras eller accepteras.

Leverantören ska vid genomförandet av riskanalyser beakta aktuella omvärldsföreteelser och inträffade incidenter som är relevanta för att upprätthålla säkerheten i nätverk och informationssystem.

Den valda riskanalysmetoden ska utgå från etablerad standard.

[20] s.40 Regeringens proposition 2017/2018:205 Informationssäkerhet för samhällsviktiga och digitala tjänster

Allmänna råd

Gruppering av nätverk och informationssystem, 4 §

Leverantören kan välja att kategorisera likvärdiga nätverk eller informationssystem och göra en riskanalys för en viss grupp så länge detta ändå innebär att samtliga aktuella nätverk och informationssystem omfattas av en relevant riskanalys.

Hot som bör analyseras, 4 §

Leverantören bör åtminstone analysera organisatoriska, logiska och fysiska hot vid genomförandet av riskanalyser.
Analys av organisatoriska hot bör åtminstone omfatta kritiska personberoenden, otillräcklig kompetensförsörjning, bristfälliga processer för att uppnå en hög säkerhet i nätverk och informationssystem (särskilt bristfälliga rutiner vid förändringshantering), bristfällig incidenthantering och bristfällig behörighets- och åtkomsthantering.
Analys av logiska hot bör åtminstone omfatta kända sårbarheter i mjukvara, logiska överbelastningsattacker, logiska intrång, otillåtna förändringar av DNS-data, konfigurationsfel, fel och brister i hårdvara eller mjukvara (såväl egenutvecklad som utvecklad av annan) samt bristfällig segmentering av nätverk. Med DNS-data avses uppgifter om bl.a. vilken IP-adress ett efterfrågat domännamn motsvarar, en officiell namnserver för en zon, parametrar för och information om zonen samt vilket domännamn som motsvarar en efterfrågad IP-adress.
Analys av fysiska hot bör åtminstone omfatta stöld, brand, kabelbrott och strömavbrott.
Riskanalyser bör innehålla planerade förändringar som kan få negativa konsekvenser på säkerheten i nätverk och informationssystem och de hot som föranlett inträffade säkerhetsincidenter som ska rapporteras i enlighet med 18 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Kvalificerade bedömningar, 4 §

Sannolikhetsbedömningar kan indelas i olika nivåer exempelvis mycket sällsynt, tämligen sällsynt, regelbundet och ofta. Konsekvensbedömningar på säkerheten i nätverk och informationssystem kan delas in i olika nivåer såsom försumbar, lindrig, måttlig, allvarlig och katastrofal.

Deltagare i riskanalysarbetet, 4 §

Leverantören bör se till att personer med relevant kunskap deltar i arbetet med riskanalys.

5 § Leverantörens dokumentation av riskanalysarbetet enligt 4 § ska innehålla:

1. en unik beteckning för varje nätverk och informationssystem som har identifierats enligt 4 §,

2. vilken funktionalitet nätverket eller informationssystemet enligt 4 § har,

3. en hänvisning till den för nätverket eller informationssystemet aktuella riskanalysen enligt 4 §,

4. den riskanalysmetod som används och

5. en redogörelse för bedömning av sannolikhet och konsekvens enligt 4 § andra stycket 2 - 5,

Leverantörens riskanalys och dokumentationen i första stycket 3 - 5 ska bevaras i fem år från det att den upprättats eller uppdaterats.

Kravet på identifiering i 4 § innebär att leverantören inledningsvis ska identifiera samtliga nätverk och informationssystem. Syftet med kravet är att leverantören ska ha en aktuell och samlad bild över samtliga nätverk och informationssystem och vilka funktioner de har. En god kontroll över denna information underlättar leverantörens vidtagande av säkerhetsåtgärder, samt andra relevanta åtgärder för att upprätthålla en hög skyddsnivå för de aktuella nätverken och informationssystemen.

Syftet med kraven gällande riskanalys (4 §) är att leverantören genom förebyggande analyser av identifierade hot kan minska risken för att incidenter inträffar och minimera konsekvenserna om dessa skulle inträffa genom att vidta lämpliga säkerhetsåtgärder. När leverantören genomför riskanalyser i enlighet med kraven kommer leverantören få underlag för bedömningen av om säkerhetsåtgärder behöver vidtas för att eliminera, reducera eller acceptera risker.

Kravet på att leverantören ska beakta sådana omvärldsföreteelser och inträffade incidenter som är relevanta för att upprätthålla säkerheten (4 §) syftar till att säkerställa att leverantören beaktar sådana händelser och incidenter som potentiellt kan få en påverkan på upprätthållandet av säkerheten hos de berörda nätverken och informationssystemen. Ett pågående omvärldbevakningsarbete är av stor vikt för att tillse att rätt hot analyseras i riskanalysen.

Syftet med kraven på dokumentation av riskanalysarbete i 5 § är att åstadkomma en systematisk uppföljning av säkerhetsarbetet och kontroll av vilka riskbedömningar som gjorts för olika delar av verksamheten. Genom kravet på framtagande av dokumenterade bedömningsgrunder säkerställs att analyserna genomförs på ett enhetligt och jämförbart sätt över tid. Att dokumentationen även ska innefatta en hänvisning till aktuella riskanalyser innebär att leverantören på ett systematiskt sätt kan ha kontroll över att

riskanalyserna genomförts för samtliga berörda nätverk och informationssystem samt att denne i efterhand snabbt kan kontrollera vilka riskbedömningar som gjorts för ett visst nätverk och informationssystem. Att dokumentationen ska sparas under en viss angiven tidsperiod möjliggör spårbarhet vad gäller tidigare identifierade och analyserade hot och anledningen till sedan tidigare vidtagna åtgärder. Det underlättar även utvärdering av tidigare riskbedömningar i syfte att bättre omhänderta risker vid uppdatering av riskanalyser.

Allmänt råd om gruppering av nätverk och informationssystem
Det allmänna rådet om att kategorisera likvärdiga nätverk eller informationssystem förtydligar och ger vägledning om att en riskanalys kan göras för en viss grupp så länge detta ändå innebär att samtliga aktuella nätverk och informationssystem omfattas av en relevant riskanalys.

Allmänt råd om hot som bör beaktas
Det tillhörande allmänna rådet till den föreslagna bestämmelsen om genomförande av riskanalys förtydligar och ger vägledning kring vilka hot som bör analyseras och andra aspekter som bör övervägas vid genomförande av riskanalys.

Allmänt råd om riskanalys särskilt vid förändringar och incidenter
Bakgrunden till det allmänna rådet om att leverantören särskilt bör genomföra riskanalyser inför planerade förändringar är att PTS har kunnat konstatera att förändringshantering är en av de vanligaste orsakerna till omfattande avbrott och störningar utifrån myndighetens erfarenheter ifrån tillsyn över telekomoperatörernas säkerhetsarbete.
Syftet med det allmänna rådet om att riskanalyser särskilt bör genomföras eller uppdateras efter säkerhetsincidenter är att leverantören bör analysera om behovet av säkerhetsåtgärder har förändrats med anledning av incidenten. Genom en sådan analys kan risken för att liknande incidenter inträffar i framtiden minskas.

Allmänt råd om kvalificerade bedömningar
Syftet med det allmänna rådet om kvalificerade bedömningar är att underlätta och förtydliga 4 §. Det allmänna rådet ger exempel på nivåer för bedömning av sannolikhet och konsekvens.

Allmänt råd om deltagare
Leverantören bör se till att personer med relevant kunskap deltar i arbetet med riskanalys.

Kostnader med anledning av allmänna råd
De allmänna råden till 4 § förtydligar och ger vägledning vid genomförande av riskanalyser och medför inga ytterligare några kostnader.

Allmänt om kostnader i 4-5 §§

Att leverantörer av samhällsviktiga tjänster ska genomföra riskanalyser följer redan av 12 § NIS-lagen. Av 5 § MSB:s informationssäkerhetsföreskrifter följer att varje leverantör ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna SS-EN-ISO/IEC27001:2017 och SS-EN-ISO/IEC27002:2017 om ledningssystem för informationssäkerhet eller motsvarande. Av 8 § i MSB:s informationssäkerhetsföreskrifter följer även att leverantörer ska ha ett dokumenterat arbetssätt för sitt informationssäkerhetsarbete som stöd för att identifiera, analysera och värdera risker för organisationens information, nätverk och informationssystem. Mot denna bakgrund bedömer PTS att de berörda leverantörerna redan har ett dokumenterat arbetssätt på plats för att arbeta med riskanalys, riskbedömning och riskhantering. Kostnaderna begränsas således till stor del av att krav på riskanalyser har funnits sedan NIS-lagen trädde i kraft den 1 augusti 2018 och att kravet sedan har förtydligats i MSB:s informationssäkerhetsföreskrifter som har gällt från och med den 1 november 2018.

Kostnader 4 §

Att leverantören kan välja riskanalysmetod innebär att leverantören kan behålla en sedan tidigare fungerande metod eller välja den metod som bäst passar verksamheten. Den valda riskanalysmetoden ska dock utgå från en etablerad standard, exempelvis SS-EN ISO/EIC 27001:2017 alternativt 27002:2017.

De administrativa engångskostnaderna torde begränsas till en eventuell revidering av sedan tidigare framtagen riskanalysmetod.

I händelse av att leverantören behöver komplettera sin befintliga riskanalysmetod uppskattar PTS att den administrativa engångskostnaden för detta uppgår till 2 500 kronor, givet en tidsåtgång om fem timmar och en lönekostnad om 500 kronor/timme.

I händelse av att leverantören behöver komplettera sina kommande riskanalyser för identifierade nätverk och informationssystem utifrån PTS föreslagna krav uppskattar PTS att det nu föreslagna kravet medför en tidsåtgång om 1 - 2 timmar per analysobjekt. Med en lönekostnad om 500 kronor/timme uppgår den administrativa engångskostnaden från 500 kronor till 1000 kronor per analysobjekt.

Utifrån en uppskattning om att leverantören har 30 stycken nätverk och informationssystem innebär detta en total tidsåtgång om 30 till 60 timmar för genomförande av riskanalys. Med en lönekostnad om 500 kronor/timme uppgår därmed den totala administrativa engångskostnaden från 15 000 kronor till 30 000 kronor för en leverantör.

Enligt det föreslagna kravet i 4 § ska leverantören även beakta omvärldsföreteelser och inträffade incidenter som är relevanta för att upprätthålla säkerheten i nätverk och informationssystem. När det gäller att ha kännedom om omvärldsföreteelser som är relevanta för säkerheten i nätverk och informationssystem förutsätter PTS att leverantören redan idag, inom ramen för tillhandahållandet av den samhällsviktiga tjänsten, bedriver omvärldsbevakning i det dagliga arbetet, med befintliga relevanta personella resurser. Omvärldsbevakning kan exempelvis ske genom att leverantören tar del av nyheter om exempelvis aktuella sårbarheter i mjukvara, nyligen genomförda logiska attacker eller andra typer av inträffade incidenter från underleverantörer såsom programvaruleverantörer, eller via anslutning till olika communities/grupperingar avseende olika sakområden (exempelvis DNS) men även från myndigheter och media. Tillgång till flera omvärldsbevakningskällor är ofta kostnadsfria. När det gäller inträffade incidenter bedömer PTS att leverantören dels genom sitt omvärldsbevakningsarbete har kännedom om relevanta incidenter hos andra aktörer, dels är det PTS uppfattning att de anmälda leverantörerna redan idag har system för dokumentation och uppföljning av inträffade incidenter i den egna verksamheten.

De årliga administrativa kostnaderna består av arbetet med årlig uppdatering av riskanalyserna samt arbetet med omvärldsbevakning. Eftersom kostnaderna för uppdatering av riskanalyser föranleds av NIS-lagens krav på årlig uppdatering av riskanalyserna (12 §) medför kravet i denna del därmed inte några ytterligare kostnader. Vad gäller årliga administrativa kostnader för omvärldsbevakning uppskattar PTS att tidsåtgången för genomförande av omvärldsbevakning i snitt uppgår till 30 timmar per år för en leverantör. Med en lönekostnad om 500 kronor/timme uppgår därmed den administrativa årliga kostnaden till 15 000 kronor för en leverantör.

PTS bedömer att de övriga kostnaderna som är förknippade med kravet avseende riskanalyser är hänförliga till personalkostnader. Dessa kostnader kan utgöras av kostnader för eventuell utbildning av personal avseende tillkommande krav med anledning av föreslagen reglering vad gäller riskanalysarbetet. Kostnaderna bedöms dock inte vara särskilt omfattande eftersom PTS förutsätter att leverantörerna redan genomför riskanalyser och att den personal som arbetar med dessa frågor därigenom får antas vara förtrogna med riskanalysarbete. De kostnader som exempelvis skulle kunna uppstå kan röra sig om att anordna ett informationsmöte eller en internutbildning om riskanalys. Det nu föreslagna kravet kan medföra en extra tidsåtgång om 1 – 2 timmar per deltagare. PTS uppskattar att en intern utbildningsinsats omfattar fyra deltagare med en lönekostnad om 500 kronor/timme vilket innebär att de övriga kostnaderna totalt uppgår till 2 000 - 8 000 kr.

Kostnader 5 §

Det uppställs inga krav på vilken form dokumentationen ska ha utan det är upp till leverantören att avgöra hur kravet ska efterlevas. Detta möjliggör att de leverantörer som redan har befintliga system eller rutiner kan behålla, eller göra

tillägg i, sina befintliga system eller rutiner för att uppfylla kravet. PTS bedömer att leverantörerna redan har identifierat och dokumenterat sina nätverk och informationssystem i viss utsträckning

Som ovan nämnts bedömer PTS att leverantörerna redan har ett dokumenterat arbetssätt för genomförandet av riskanalyser och riskanalysmetod då detta följer av MSB:s informationssäkerhetsföreskrifter. De föreslagna kraven på dokumentation innebär dock att inte bara arbetssättet ska dokumenteras utan även riskanalysmetoden, bedömningar av sannolikhet och konsekvens, och den för nätverket eller informationssystemet aktuella riskanalysen. Kravet innebär därmed krav på ytterligare dokumentation jämfört med MSB:s informationssäkerhetsföreskrifter. Vidare ska dokumentationen i vissa delar sparas i fem år.

Kravet i 5 § kan medföra administrativa engångskostnader för dokumentation av den vid behov reviderade riskanalysmetoden, dokumentation av bedömningar enligt 4 § andra stycket 2 - 5 för bedömningen att eliminera, reducera eller acceptera en risk i enlighet med 4 § fjärde stycket samt hänvisning till den för nätverket eller informationssystemet aktuella riskanalysen.
De administrativa engångskostnaderna som är förknippade med kraven kan således avse upprättande av den dokumentation som krävs och eventuell justering av redan befintlig dokumentation. PTS beräknar att tidsåtgången för den tillkommande dokumentationen i snitt tar en timme per analysobjekt. För 30 analysobjekt uppgår den totala tidsåtgången till 30 timmar. PTS uppskattar därmed att de administrativa engångskostnaderna för olika typer av dokumentation med anledning av riskanalysarbetet uppgår till 15 000 kronor utifrån en lönekostnad om 500 kronor/timme samt en tidsåtgång för arbetet om 30 timmar.

Kravet på att viss dokumentation ska bevaras i fem år kan medföra årliga administrativa kostnader för det fall leverantören i nuläget inte sparar denna information under så lång tid. PTS bedömer att det i snitt tar två timmar per år att spara ned dokumentationen på valfritt och lämpligt sätt. Med en lönekostnad om 500 kronor/timme uppgår den totala årliga administrativa kostnaden till 1 000 kr.

4.4 Åtgärder 6 §

6 § Om riskbedömningen påvisar risker som bör elimineras eller reduceras ska leverantören vidta åtgärder för att hantera riskerna i enlighet med vad som föreskrivs i 8 – 16 §§ nedan. Leverantören ska därutöver vidta de ytterligare åtgärder som är nödvändiga för att hantera de risker som framkommit i riskbedömningen. Samtliga åtgärder ska vidtas på en nivå som är proportionerlig i förhållande till den föreliggande risken. I den bedömningen ska leverantören beakta samtliga tekniska lösningar som vid var tid finns tillgängliga på marknaden.

Nu föreslaget krav förtydligar 12 § NIS-lagen. Kravet lämnar ett utrymme för leverantörerna att själva avgöra vilka säkerhetsåtgärder som är lämpliga och proportionella i förhållande till analyserad risk. Bestämmelsen innebär således att det är leverantörens riskanalys som avgör om och i sådana fall vilka säkerhetsåtgärder som behöver vidtas.

PTS har angett ett antal säkerhetsåtgärder i 8 - 16 §§ som ska vidtas om leverantören i sin riskbedömning kommer fram till att det finns vissa angivna risker som ska elimineras eller i någon mån reduceras. Har riskbedömningen exempelvis visat risker som behöver elimineras eller i vart fall reduceras vad gäller hantering och tilldelning av behörighet, ska leverantören vidta åtgärder i enlighet med föreskriftskravet om behörighetshantering.

Bestämmelsen innebär vidare att leverantören ska vidta säkerhetsåtgärder som denne efter genomförandet av riskanalyser i övrigt bedömer vara nödvändiga för att hantera identifierade risker. De säkerhetsåtgärder som leverantören i övrigt ska vidta efter genomförd riskanalys, utgörs således av sådana säkerhetsåtgärder som inte specifikt anges i föreskrifterna.

Kravet innebär att leverantören vid bedömningen av vad som är att se som en lämplig nivå i förhållande till risken ska beakta den senaste tekniska utvecklingen. Detta innebär att leverantören måste hålla sig uppdaterad om de tekniska lösningar som finns på marknaden då teknisk utveckling kan medföra att behovet av säkerhetsåtgärder förändras.

Syftet med kravet på vidtagande av säkerhetsåtgärder är att se till att leverantören vidtar åtgärder som säkerställer en nivå på säkerheten som är lämplig i förhållande till risken. Vidtagande av lämpliga säkerhetsåtgärder är enligt PTS bedömning också en grundförutsättning för ett långsiktigt, kontinuerligt och systematiskt informationssäkerhetsarbete. Utan vidtagande av förebyggande säkerhetsåtgärder finns det, enligt PTS bedömning, en risk att säkerhetsarbetet blir alltför reaktivt, dvs. att åtgärder endast vidtas efter det att en incident inträffat. Enligt PTS bedömning är det nödvändigt att säkerhetsarbetet i stor utsträckning bedrivs proaktivt, så att hot mot säkerheten i nätverk och informationssystem så långt det är rimligt hanteras innan det att en incident inträffat.

Kostnader 6 §

PTS bedömning är att leverantörerna genomför riskanalyser och vidtar säkerhetsåtgärder redan idag. Kostnaderna som är förenade med nu föreslagna föreskrifter begränsas därmed till viss del av att krav på vidtagande av säkerhetsåtgärder redan finns i 12-14 §§ NIS-lagen och i MSB:s informationssäkerhetsföreskrifter.

Det nu föreslagna kravet om att bevaka de tekniska lösningar som finns tillgängliga torde inte medföra några kostnader då PTS förutsätter att en sådan bevakning redan genomförs. I den utsträckning leverantören inte redan beaktar

tekniska lösningar i sin proportionalitetsbedömning kan dock årliga administrativa kostnader enligt följande uppstå. PTS uppskattar att tidsåtgången för att bevaka de tekniska lösningar som finns på marknaden vid var tid skulle kunna uppgå till ca 40 timmar per år. Detta innebär då en årlig kostnad om 20 000 kr utifrån en lönekostnad om 500 kronor/timme.

Beroende på vilka hot som vid var tid föreligger och nivån av skydd leverantören har idag, kan kraven i de föreslagna föreskrifterna innebära allt från små till mycket stora investeringar i säkerhetsåtgärder. PTS kan således inte kvantifiera eller uppskatta kostnaderna fullt ut mot bakgrund av att det inte är möjligt att i förväg veta vilka investeringar som respektive leverantör kommer att behöva göra efter genomförda riskanalyser. PTS kommer att uppskatta de kostnader som nu föreslagna krav om säkerhetsåtgärder i 8-16 §§ kan föranleda, se avsnitt 4.5.

4.5 Åtgärdsplan 7 §

7 § Åtgärderna ska dokumenteras i en åtgärdsplan som bevaras under fem år från det att den upprättats eller uppdaterats. Av åtgärdsplanen ska framgå följande:

1. valet av åtgärd,

2. för vilket nätverk eller informationssystem åtgärden vidtas,

3. vilka risker som respektive åtgärd avser att hantera,

4. en motivering till valet av åtgärd,

5. sedan tidigare genomförda åtgärder och hanterade risker,

6. vem som är ansvarig för att vidta åtgärden,

7. när åtgärden ska vara genomförd samt

8. när åtgärden har vidtagits.

Leverantören ska följa upp och utvärdera vidtagna åtgärder vid behov.

Kravet innebär att de säkerhetsåtgärder som leverantören kommer att vidta ska framgå av en åtgärdsplan. Den nu föreslagna bestämmelsen förtydligar åtgärdsplanens innehåll och de delar som ska ingå i åtgärdsplanen.

Genom åtgärdsplanen struktureras leverantörens arbete med att vidta säkerhetsåtgärder så att det blir tydligt vad som ska genomföras, varför åtgärden ska genomföras, när åtgärden ska genomföras och vem som ansvarar för att vidta åtgärden.

Kravet på dokumentation av åtgärdsplanen framgår direkt av 12 § NIS-lagen och utgör en förutsättning för uppföljning av det systematiska, förebyggande informationssäkerhetsarbetet, och kontroll av om och vilka säkerhetsåtgärder som har vidtagits eller ska vidtas. Det nu föreslagna kravet om att dokumentationen ska sparas i fem år möjliggör en spårbarhet, vilket underlättar för leverantören att kontrollera vilka åtgärder som vidtagits även efter att en viss tid har förflutit.

Kostnader 7 §

Att leverantörer av samhällsviktiga tjänster ska ta fram en åtgärdsplan följer redan av 12 § NIS-lagen. Kostnaderna som är förenande med nu föreslagna föreskrifter begränsas också till viss del av att krav på att ha ett systematiskt och riskbaserat informationssäkerhetsarbete redan följer av MSB:s informationssäkerhetsföreskrifter. PTS bedömning är därför att leverantörerna redan idag har en eller flera åtgärdsplaner för sina nätverk och informationssystem med uppgifter om de säkerhetsåtgärder som behöver vidtas, vem som ansvarar för att åtgärderna vidtas och när åtgärderna ska vidtas, men att vissa ytterligare uppgifter behöver ingå.

Den administrativa engångskostnaden torde begränsas till en eventuell revidering av sedan tidigare framtagen åtgärdsplan.

I händelse av att leverantören kommer att behöva komplettera sin kommande åtgärdsplan uppskattar PTS att de administrativa engångskostnaderna per nätverk/informationssystem uppgår till 1500 kr givet en lönekostnad om 500 kronor/timme samt en tidsåtgång för arbetet om 3 timmar.

Utifrån en uppskattning om att leverantören har 30 stycken nätverk och informationssystem uppgår den totala administrativa engångskostnaden till 45 000 kronor.

De årliga administrativa kostnaderna för uppdatering av åtgärdsplanen är förenade med kraven i NIS-lagen samt MSB:s informationssäkerhets-föreskrifter. Detta krav medför således inga ytterligare kostnader.

Kravet på att åtgärdsplaner ska bevaras i fem år kan medföra årliga administrativa kostnader för det fall leverantören i nuläget inte sparar denna information under så lång tid. PTS bedömer att det i snitt tar två timmar per år att spara ned dokumentationen på valfritt och lämpligt sätt. Med en lönekostnad om 500 kronor/timme uppgår den totala årliga administrativa kostnaden till 1 000 kr.

PTS bedömer att de övriga kostnaderna som är förknippade med kravet kan vara hänförliga till personalkostnader. Dessa kostnader kan utgöras av kostnader för eventuell utbildning av personal avseende tillkommande krav med anledning av föreslagen reglering vad gäller åtgärdsplanen. Kostnaderna bedöms dock inte vara särskilt omfattande eftersom PTS förutsätter att

leverantörerna redan tar fram åtgärdsplaner och att den personal som arbetar med dessa frågor därigenom får antas vara förtrogna med arbetet. De kostnader som skulle kunna uppstå kan röra sig om att anordna ett informationsmöte eller en internutbildning. Det nu föreslagna kravet uppskattas medföra en extra tidsåtgång om 1 – 2 timmar per deltagare och utbildningstillfälle. Om den interna utbildningsinsatsen omfattar 5 deltagare med en lönekostnad om 500 kronor/timme uppgår kostnaden totalt till 2 500 – 5 000 kr.

4.5.1 Fysiska och logiska skydd 8 §

8 § Leverantören ska, i den utsträckning som följer av 6 §, vidta åtgärder för att upprätthålla ett effektivt skydd av säkerheten i nätverk och informationssystem mot brister i fysiskt och logiskt skydd. Åtgärderna ska ge skydd mot logiska intrång, logiska överbelastningsattacker och andra identifierade logiska hot.

Allmänna råd
Fysiska och logiska skydd, 8 §
Andra identifierade logiska hot är externa och interna hot som exempelvis kan leda till manipulation av DNS-data och resursblockering.

Åtgärderna bör även omfatta skydd mot logiska hot i den egna verksamheten, såsom hot som leder till obehörig åtkomst till DNS-data, autentiseringsuppgifter, tilldelade behörigheter, loggningsinformation och krypteringsnycklar.

Kravet innebär att leverantören ska skydda nätverk och informationssystem mot brister i såväl fysiskt som logiskt skydd utifrån vad som framkommit i leverantörens genomförda riskbedömning. Vilka åtgärder som konkret ska vidtas framgår inte av föreskrifterna.

När det gäller skydd mot fysiska intrång kan det innebära att leverantören genom skalskydd, tillträdeskontroll, inbrottslarm, kanalisation och andra fysiska hinder ser till att någon inte obehörigen får tillträde.

När det gäller skydd mot logiska hot kan det innebära att leverantören ska vidta åtgärder för att förhindra att logiska incidenter inträffar, se avsnitt 2.2 Omvärldsbild och närmare om problemen.

Syftet med kravet är att leverantören ska skydda sina nätverk och informationssystem mot avsiktliga och oavsiktliga angrepp eller mot att andra omständigheter med potentiell negativ inverkan på säkerheten i nätverk och informationssystem uppstår. Dels ska leverantören se till att skydda sina nätverk och informationssystem mot att exempelvis en enskild individ, utan avancerade verktyg, relativt snabbt kan orsaka skador på tillgångar som medför incidenter i nätverk och informationssystem. Dels ska leverantören skydda sina nätverk och informationssystem mot att någon person eller något system obehörigt tar sig in i informationssystem och förorsakar förvanskning, förlust eller stöld av information, exempelvis DNS- eller autentiseringsuppgifter.

Att leverantören har vidtagit säkerhetsåtgärder för att hantera den här typen av hot utgör en förutsättning för att leverantören på ett förebyggande och systematiskt sätt har möjlighet att hantera fysiska och logiska incidenter. Utan förebyggande åtgärder finns en uppenbar risk att leverantören endast agerar mer reaktivt när t.ex. ett intrång eller överbelastningsattack redan inträffat.

Kostnader 8 §

När det gäller kostnader som föranleds av förslaget på krav är storleken på kostnaderna beroende på resultatet av riskanalysen, vilken nivå av skydd som leverantören har idag samt leverantörens arbete med att åtgärda identifierade risker, se även avsnitt 4.1.2.

Exempel på åtgärder som leverantören skulle kunna vidta omfattar investering i utrustning för intrångsdetektering, redundans av vissa informationssystem och nätverk, filtrering av oönskad trafik till informationssystemen samt autentisering av användare och system innan åtkomst till informationssystem och nätverk medges.

Ytterligare exempel på investeringar som kan komma att krävas efter riskbedömning är anskaffning av ytterligare internetanslutningstjänster med tillräcklig kapacitet till den samhällsviktiga tjänsten från fler leverantörer som ger ett utökat logiskt skydd. Ett annat exempel är investering i en tjänst där flera identiska namnservrar tilldelas samma IP-adress som då kan dela på arbetet med att besvara DNS-frågor (anycast). Antalet namnservrar kan mångfaldigas varvid en bättre geografisk spridning är möjlig att uppnå. Det kan också handla om investering i ny hård- och mjukvara med utökad funktionalitet och kapacitet för att exempelvis ha ett bättre skydd mot resursblockering.

Kostnaderna för åtgärderna är avpassade till den aktuella verksamhetens behov. Efter undersökning av priser kan PTS konstatera att prisuppgifter för åtgärder många gånger lämnas i offert på begäran av leverantör, varför PTS inte kan redogöra för ett exempel på kostnader för investering.

De årliga administrativa kostnaderna för kravet skulle kunna bestå i fortsatta bedömningar av vilka investeringar som ska göras avseende fysiska och logiska skydd. PTS uppskattar att årliga administrativa kostnader uppgår till 15 000 kronor, givet en tidsåtgång om 30 timmar och en lönekostnad om 500 kronor/timme.

PTS bedömer att de övriga kostnaderna utöver investeringar som är förknippade med detta krav är hänförliga till personalkostnader, främst kostnader för eventuell utbildning av personal i de nya fysiska och logiska skydd som har anskaffats enligt kravet så att berörda är insatta i dessa. Det nu föreslagna kravet uppskattas medföra en extra tidsåtgång om 1 – 2 timmar per deltagare och utbildningstillfälle. Om den interna utbildningsinsatsen omfattar 4 deltagare med en lönekostnad om 500 kronor/timme uppgår kostnaden totalt till 2 000 – 4 000 kr.

Kostnader för allmänt råd

Det tillhörande allmänna rådet till den föreslagna bestämmelsen om fysiska och logiska skydd (8 §) medför inga merkostnader utöver de kostnader som följer av föreslaget krav då det föreslagna allmänna rådet endast förtydligar bestämmelsen.

4.5.2 Säker programvaruhantering 9 §

10 § Leverantören ska, i den utsträckning som följer av 6 §, vidta åtgärder för att säkerställa att kända allvarliga brister eller sårbarheter i informationssystemens programvara omhändertas (säker programvaruhantering). Leverantören ska ha dokumenterade processer och rutiner för säker programvaruhantering.

Allmänna råd
Säker programvaruhantering, 9 §
Processerna och rutinerna för säker programvaruhantering bör åtminstone omfatta hantering av operativsystem och applikationsprogram. Leverantören bör regelbundet och vid behov genomföra säkerhetsuppdateringar av programvara för informationssystem.

Kravet innebär att leverantören ska vidta åtgärder avseende säker programvaruhantering utifrån vad som framkommit i leverantörens genomförda riskbedömning. Vilka åtgärder som konkret ska vidtas framgår inte av föreskrifterna.

Syftet med bestämmelsen är att se till att programvaruhantering inte ger upphov till incidenter eller leder till bristfällig implementering. När tekniken implementeras på ett bristfälligt (t.ex. ogenomtänkt eller otillräckligt) sätt kan brister och sårbarheter uppstå i programvara, vilket kan utnyttjas av antagonister. Säkerheten i nätverk och informationssystem blir inte starkare än den svagaste länken. Det är därför viktigt att programvaror i informationssystem som används för att tillhandahålla den samhällsviktiga tjänsten är moderna, säkra och uppdaterade. Det är även viktigt att det inte råder brister i leverantörens rutiner för att kunna bedriva ett systematiskt underhåll och uppdateringar av programvaror.

Kostnader 9 §

När det gäller kostnader som föranleds av förslaget är storleken på kostnaderna beroende på vilken nivå av skydd som leverantören har idag samt leverantörens arbete med att åtgärda identifierade risker, se även avsnitt 4.1.

PTS förutsätter att samtliga leverantörer redan idag tillämpar processer och rutiner för säker programvaruhantering samt att dessa processer och rutiner till viss del finns dokumenterade. I händelse av att leverantören behöver se över och komplettera sin process för säker programvaruhantering samt komplettera

dokumentationen över detsamma uppskattar PTS att de administrativa engångskostnaderna uppgår till 5 000 kronor givet en lönekostnad om 500 kronor/timme och en tidsåtgång för arbetet om tio timmar.

I händelse av att leverantören behöver anskaffa ett system för centraliserad och automatiserad sårbarhetsbedömning och distribution av uppdateringar, bedömer PTS att installation och test av den nya programvaran medför en administrativ engångskostnad, som kan medföra en tidsåtgång om fyra timmar för installation och fem timmar för test av den nya programvaran. Detta medför en administrativ engångskostnad om 4 500 kronor givet en lönekostnad om 500 kronor/timme.

System för centraliserad och automatiserad sårbarhetsbedömning och distribution av uppdateringar som kan behöva införskaffas för att komplettera leverantörens säkerhetsnivå finnas på marknaden som opensource-programvara och är därmed gratis.

Kostnader för allmänt råd

Det tillhörande allmänna rådet till den föreslagna bestämmelsen om säker programvaruhantering (9 §) förtydligar och ger vägledning kring aspekter som gäller säker programvaruhantering. Det allmänna rådet medför inga merkostnader utöver de kostnader som följer av föreslaget krav då det föreslagna allmänna rådet endast förtydligar bestämmelsen.

4.5.3 Fysisk och logisk behörighets- och åtkomsthantering 10-11 §§

10 § Leverantören ska, i den utsträckning som följer av 6 §, upprätta och tillämpa processer och rutiner för tilldelning, ändring, återkallande och uppföljning av behörigheter. Uppföljning av tilldelade behörigheter ska ske löpande samt vid behov. Tilldelade behörigheter ska dokumenteras och hållas uppdaterade.

11 § Leverantören ska, i den utsträckning som följer av 6 §, vidta åtgärder för att säkerställa att endast den person eller de system som är behöriga ska medges åtkomst till nätverk och informationssystem. Sådan behörighet ska begränsas till vad som är nödvändigt för syftet med åtkomsten och avse fysisk och logisk åtkomst där så är tillämpligt.

Allmänna råd
Åtkomsthantering, 11 §
Leverantören bör skapa unika identiteter för de personer och system som är behöriga till nätverk och informationssystem.

Flerfaktorsautentisering bör användas vid åtkomst till informationssystem från externa nätverk.

Kraven innebär att leverantören ska vidta åtgärder avseende fysisk och logisk behörighets- och åtkomsthantering utifrån vad som framkommit i

leverantörens genomförda riskbedömning. Vilka åtgärder som konkret ska vidtas framgår inte av föreskrifterna.

Syftet med bestämmelserna är att leverantören ska säkerställa att nätverk och informationssystem skyddas från obehörig åtkomst så att endast den person eller de system som är behöriga ska medges åtkomst. Det finns alltid en risk att obehöriga får åtkomst till nätverk och informationssystem och därigenom kan orsaka skada. Skalskydd, tillträdeskontroll och kabelskydd är exempel på säkerhetsåtgärder som begränsar fysisk åtkomst till nätverk och informationssystem. Exempel på åtgärder för att begränsa logisk åtkomst är brandväggar, autentisering av användare samt upprättande av unika identiteter (användarkonton) med tilldelade anpassade behörigheter beroende av behörighetsbehov hos användarna.

Tilldelning, ändring, återkallande och uppföljning av behörigheter ska följa rutiner som säkerställer att förekommande behörigheter hålls aktuella samt är i enlighet med vad som är nödvändigt för syftet med åtkomsten. Förändringar som sker i organisationen, exempelvis att en person byter roll alternativt avslutar sin tjänst ska återspeglas i personens innehav av behörigheter.

Kravet på att tilldelade behörigheter ska dokumenteras och kravet på en dokumenterad rutin för tilldelning, ändring, återkallande och uppföljning av tilldelade behörigheter utgör en förutsättning för ett systematisk och långsiktigt säkerhetsarbete och för uppföljning och kontroll av vilka behörigheter som tilldelats för olika delar av verksamheten.

PTS bedömning är att de flesta leverantörerna har någon form av behörighets- och åtkomsthanteringsrutiner, även om dessa inte nödvändigtvis utgörs av formella och dokumenterade processer/rutiner.

Allmänna råd om åtkomsthantering

Det tillhörande allmänna rådet förtydligar och ger vägledning kring aspekter om fysisk och logisk behörighets- och åtkomsthantering. Även detta råd syftar till att skydda nätverk och informationssystem från obehörig åtkomst.

Av det allmänna rådet följer att leverantörerna bör skapa unika identiteter för de personer och system som är behöriga till nätverk och informationssystem samt att flerfaktorsautentisering bör användas i vissa angivna fall. Syftet med rådet är att skydda informationssystem från obehörig åtkomst.

Kostnader 10-11 §§

När det gäller kostnader som föranleds av förslaget på krav är storleken på kostnaderna beroende på vilken nivå av skydd som leverantören har idag samt leverantörens arbete med att åtgärda identifierade risker, se även avsnitt 4.1.

PTS förutsätter att samtliga leverantörer redan idag tillämpar processer och rutiner för fysisk och logisk behörighets- och åtkomsthantering samt att dessa processer och rutiner till viss del finns dokumenterade.

De administrativa engångskostnader som kan uppstå är i det fall leverantörerna behöver komplettera sin dokumentation av processer och rutiner som rör fysisk och logisk behörighets- och åtkomsthantering. Det kan exempelvis röra sig om bedömning av vilka behörigheter som ska tilldelas till vem/vilket system. Dessutom kan kravet innebära kostnader för dokumentation av behörigheter samt vidareutveckling och dokumentation av processen för tilldelning, ändring och uppföljning av tilldelade behörigheter.

I det fall leverantören behöver komplettera sina befintliga dokumenterade processer och rutiner för fysisk och logisk behörighets- och åtkomsthantering uppskattar PTS att de administrativa engångskostnaderna för detta uppgår till 3000 kronor, givet en tidsåtgång om 6 timmar och lönekostnad om 500 kronor/timme.

De årliga administrativa kostnaderna för kravet skulle kunna bestå i fortsatta bedömningar av vilka behörigheter som ska tilldelas, samt av ändringar och uppföljningar av tilldelade behörigheter och fortsatt dokumentation enligt kravet. PTS uppskattar att årliga administrativa kostnader uppgår till 15 000 kronor, givet en tidsåtgång om 30 timmar och en lönekostnad om 500 kronor/timme.

PTS bedömer att de övriga kostnaderna som är förknippade med detta krav är hänförliga till personalkostnader, främst kostnader för eventuell utbildning av personal i processer och rutiner som ska tas fram enligt kravet så att berörda är insatta i dessa. Det nu föreslagna kravet uppskattas medföra en extra tidsåtgång om 1 – 2 timmar per deltagare och utbildningstillfälle. Om den interna utbildningsinsatsen omfattar 4 deltagare med en lönekostnad om 500 kronor/timme uppgår kostnaden totalt till 2 000 – 4 000 kr.

Kostnader för allmänna råd

I det fall leverantören väljer att införa flerfaktorsautentisering vid åtkomst till informationssystem kan detta medföra ytterligare administrativa och övriga kostnader. Kostnaderna för två- eller flerfaktorsautentisering är, som i många fall, beroende på vilken lösning som väljs och i vilken utsträckning leverantören själv med egen verksamhet kan ta fram en lösning.

Administrativa kostnader kan handla om administration, skydd och förvaltning av de ytterligare autentiseringsuppgifter och informationssystem som krävs med anledning av multifaktorsautentiseringslösningen samt eventuell användarsupport. I det fall leverantören genom sin riskanalys kommer fram till att denna behöver införa flerfaktorsautentisering, uppskattar PTS att den administrativa engångskostnaden, innefattande installation, testning och

användarsupport, uppgår till 15 000 kronor, givet en tidsåtgång för arbetet om 30 timmar och en lönekostnad om 500 kronor/timme.

Övriga kostnader skulle kunna utgöras av anskaffning av viss ny hårdvara, mjukvara eller en tjänst. I det fall lösningen köps in kan kostnaden uppgå till ca 1 000 kronor per användare och år. Det finns även lösningar baserade på molntjänster, SMS och applikationer till mobiltelefoner som i många fall har en betydligt lägre prisbild. Det finns dessutom t.ex. lösningar med brandväggar med VPN-funktion och stöd för multifaktorautentisering att tillgå för under 20 000 SEK, men det är inte osannolikt att det slutliga priset för den enskilda aktören uppgår till mycket mer.

4.5.4 Hantering av planerade tekniska och organisatoriska förändringar 12 §

12 § Leverantören ska, i den utsträckning som följer av 6 §, genomföra relevanta tester och andra kvalitetskontroller inför och efter sådana tekniska eller organisatoriska förändringar som kan få negativa konsekvenser på säkerheten i nätverk och informationssystem. Leverantören ska ha en process för planerade förändringar som utgår från etablerad standard på området.

Inför förändringar enligt första stycket ska leverantören planera för att återställa nätverk och informationssystem i händelse av att förändringen misslyckas eller ger upphov till en incident. Planerna för återställande ska dokumenteras.

Allmänna råd
Förändringshantering, 12 §

Tekniska förändringar som kan få negativa konsekvenser på säkerheten i nätverk och informationssystem kan exempelvis vara driftsättning, migrering eller förändrad konfiguration av informationssystem, genomförande av uppdateringar av programvara, ny- och vidareutveckling av programvara samt nätverk som ansluts, förändras eller tas bort.

Organisatoriska förändringar som kan få negativa konsekvenser på säkerheten i nätverk och informationssystem kan exempelvis vara konsolidering av bolag och verksamheter och utkontraktering av tjänster.

Kravet innebär att leverantören ska vidta åtgärder för att kunna genomföra tester och kontroller inför och efter tekniska förändringar i enlighet med vad som framkommit i leverantörens genomförda riskbedömning. Det uppställs inte något krav på formen för planerna för återställande, men dessa ska vara relevanta. Det blir således leverantörens riskanalys för den planerade förändringen som avgör om ett test eller en plan för återställande behövs, samt vilket sorts test eller andra kvalitetskontroller som i förekommande fall ska genomföras och vad som ska omfattas av planerna för återställande.

Genomförande av förändringar i nätverk och informationssystem är något som är vanligt förekommande och som bör ske för att upprätthålla den samhällsviktiga tjänstens kvalitet och tillgänglighet. Tekniska och organisatoriska förändringar är dock en av de vanligaste orsakerna till incidenter. Lyckade förändringar i nätverk och informationssystem är bl.a. beroende av etablerade och ändamålsenliga processer för förändringsarbetet och, vid större förändringsarbeten, att erforderliga tester har genomförts och att leverantören har planerat för att hantera eventuella incidenter. Syftet med bestämmelsen är att motverka incidenter som kan uppstå i samband med leverantörens förändringshantering.

Kravet på dokumentation syftar till att säkerställa att förändringsarbeten kan ske på ett säkert och tillförlitligt sätt. Dessutom kan dokumentation minska personberoenden i arbetet med förändringar i nätverk och informationssystem.

Allmänt råd om förändringshantering

Det föreslagna tillhörande allmänna rådet till 12 § förtydligar och ger vägledning kring aspekter av vilka typer av tekniska och organisatoriska förändringar som kan anses få negativ påverkan på säkerheten.

Kostnader 12 §

När det gäller kostnader som föranleds av förslaget på krav är storleken på kostnaderna beroende på vilken nivå av skydd som leverantören har idag samt leverantörens arbete med att åtgärda identifierade risker, se även avsnitt 4.2.1.

PTS förutsätter att samtliga leverantörer redan idag arbetar med förändringshantering och att framtagna återställandeplaner till viss del är dokumenterade.

De administrativa engångskostnaderna kan avse kostnader för framtagande av en process för förändringshantering. Bristande dokumentation kan även medföra kostnader. I det fall leverantören inte har dokumenterade processer, skulle en administrativ engångskostnad kunna uppstå.

PTS uppskattar att administrativa engångskostnader uppgår till 5 000 kronor, givet att leverantörens arbete med att ta fram eller komplettera sina processer för förändringsarbete tar tio timmar och en lönekostnad om 500 kronor/timme.

PTS bedömer att de övriga kostnaderna som är förknippade med detta krav är hänförliga till personal- eller investeringskostnader. Det kan exempelvis handla om kostnader för eventuell utbildning av personal så att berörda är insatta i processen om förändringshantering.

I det fall leverantören behöver genomföra en utbildningsinsats uppskattar PTS att de övriga kostnaderna uppgår till 10 000 kronor, givet att utbildningen tar 4 timmar, 5 deltagare ska utbildas, och lönekostnaden är 500 kronor/timme.

Kostnader för allmänna råd

Det allmänna rådet medför inga kostnader utöver de kostnader som följer av föreslaget krav då det föreslagna allmänna rådet endast förtydligar bestämmelsen.

4.5.5 Säkerställande av kompetens och personella resurser 13 §

13 § Leverantören ska, i den utsträckning som följer av 6 §, säkerställa

1. att de som utför arbetsuppgifter för att upprätthålla säkerheten i nätverk och informationssystem har tillräcklig kompetens för att utföra sina arbetsuppgifter,

2. att tillräckliga personella resurser finns tillgängliga för att upprätthålla säkerheten i nätverk och informationssystem, och

3. att anställda och uppdragstagare känner till och tillämpar framtagna processer och rutiner för upprätthållande av säkerheten i nätverk och informationssystem.

Allmänna råd
Fortbildning inom DNS och säkerhetsåtgärder

De av leverantörens anställda som har till arbetsuppgift att arbeta med nätverk och informationssystem bör kontinuerligt fortbildas inom DNS och säkerhetsåtgärder i takt med omvärldskrav och omvärldsförändringar, till exempel DNS-mjukvaror, information om hot och nya säkerhetslösningar.

Kravet innebär att leverantören ska vidta åtgärder för att säkerställa att tillräcklig kompetens och personella resurser finns tillgängliga för att upprätthålla säkerheten i nätverk och informationssystem, utifrån vad som framkommit i leverantörens genomförda riskbedömning.

PTS tidigare erfarenhet från tillsyn inom driftsäkerhetsområdet inom telekommarknaden är att den mänskliga faktorn är en vanlig orsak till brister i säkerheten i tjänster, som kan ge upphov till incidenter (se även avsnitt 2.2 Omvärldsbeskrivning och närmare om problemen). Exempel på när den mänskliga faktorn lett till brister i säkerheten är handhavandefel och otillräckliga tekniska lösningar, t.ex. brister i arkitekturen för nätverk och informationssystem, bristfällig implementering och konfigurering, bristfällig funktionstestning och avsteg från tillämpning av interna processer och rutiner. Syftet med kravet är att säkerställa att säkerheten i nätverk och informationssystem upprätthålls.

En nyckelfråga för att upprätthålla säkerheten i nätverk och informationssystem är personalens kompetens avseende upprättande av en säker och robust DNS-

infrastruktur. Vidare är det nödvändigt med kompetens om informationssäkerhet och uppbyggnad av leverantörens nätverk och informationssystem på ett säkert sätt. Om en viss specifik kompetens är personberoende hos leverantören innebär detta en organisatorisk risk och sårbarhet. Antalet personer med rätt kompetens är därför kritiskt då det annars kan leda till att arbetsmängden för en enskild person blir övermäktig eller att leverantören kan stå utan rätt kompetens vid exempelvis avgång eller sjukfrånvaro. Kraven på att leverantören ska säkerställa att anställda och uppdragstagare känner till och tillämpar framtagna processer och rutiner för upprätthållande av säkerheten i nätverk och informationssystem bidrar till ett minskat personberoende.

Allmänt råd om fortbildning inom DNS och säkerhetsåtgärder

Det allmänna rådet innebär att leverantören löpande bör fortbilda berörda anställda inom säkerhetsaspekter och om DNS.

Kostnader 12 §

När det gäller kostnader som föranleds av förslaget på krav är storleken på kostnaderna beroende på resultatet av riskanalysen, på personalens antal och kompetens idag samt personalens kännedom och tillämpning av processer och rutiner, se även avsnitt 4.1.2.

Administrativa engångskostnader som kravet kan komma att ge upphov till är de eventuellt ytterligare åtgärder som leverantören behöver vidta för att personal ska känna till och tillämpa framtagna processer och rutiner för upprätthållande av säkerheten i nätverk och informationssystem. Det kan exempelvis handla om att anordna ett informationsmöte eller en internutbildning, eller att tillgängliggöra processer och rutiner på lämpligt sätt på intranätet.

Övriga kostnader som kan uppkomma med anledning av föreslaget krav kan handla om att upphandla konsulttjänster med en viss specifik kompetens, anställa ytterligare personal eller kompetensutveckling.

Ett exempel på övrig kostnad som kan uppkomma med anledning av kravet är i det fall en anställd behöver utbildas inom DNS via en extern kurshållare. Kostnaden för en DNS-utbildning om tre dagar kan uppgå till 26 000 kronor för en deltagare.

Kostnader för allmänna råd

Det föreslagna tillhörande allmänna rådet till 12 § förtydligar och ger vägledning kring aspekter av kompetens och tillräckliga personella resurser. Det allmänna rådet medför inga kostnader utöver de kostnader som följer av förslaget krav då det föreslagna allmänna rådet endast förtydligar bestämmelsen.

4.5.6 Spårbarhet 14 §

15 § Leverantören ska, i den utsträckning som följer av 6 §, dokumentera (logga)

1. all förändring av sådana uppgifter som är nödvändiga för upprätthållandet av säkerheten i nätverk och informationssystem så att det framgår vem som har vidtagit vilken åtgärd vid vilken tidpunkt,
2. alla systemhändelser i syfte att kunna utreda logiska intrång så att det åtminstone framgår vilka åtgärder som har vidtagits och vid vilken tidpunkt, samt

3. all läsning av sådana uppgifter som är konfidentiella.

Leverantören ska upprätta processer och rutiner för sådan loggning som framgår av första stycket. Rutinerna och processerna ska dokumenteras och hållas uppdaterade.

Leverantören ska kontrollera sådan loggning som framgår av första stycket åtminstone vid misstanke om att en incident har inträffat.

Sådana loggar som framgår av första stycket ska bevaras under åtminstone fem år.

Allmänna råd
Uppgifter som är nödvändiga för upprätthållandet av säkerheten i nätverk och informationssystem, 14 §

Med ”sådana uppgifter som är nödvändiga för upprätthållandet av säkerheten i nätverk och informationssystem” avses exempelvis DNS-data, autentiseringsuppgifter och behörigheter.

Allmänt råd om systemhändelser, 14 §

Med systemhändelser avses exempelvis händelser som involverat system och applikationer, liksom läsning, kopiering, ändring och utplåning av uppgifter i nätverk och informationssystem.

Allmänt råd om sådana uppgifter som är konfidentiella, 14 §

Med ”sådana uppgifter som är konfidentiella” avses exempelvis autentiseringsuppgifter och krypteringsnycklar.

Allmänt råd om innehållet i loggarna, 14 §

Loggarna bör innehålla information om användarkonto, systemaktiviteter, datum, tider och övriga uppgifter om intrång, lyckade och misslyckade åtkomstförsök till informationssystem, data och andra resurser, förändringar i systemkonfiguration, användning av priviligierad åtkomst, åtkomst till filer och typ av åtkomst, nätverksadresser och protokoll.

Kravet innebär att leverantören ska vidta åtgärder som rör loggning utifrån vad som framkommit i leverantörens genomförda riskbedömning och i enlighet med föreslaget krav, se även avsnitt 4.1.2.

Syftet med kravet är att leverantören ska kunna utreda händelser eller inträffade incidenter i efterhand, dvs. vad som har hänt, när och av vem (person eller system).

PTS förutsätter att leverantörerna redan idag har samt tillämpar processer och rutiner avseende loggning samt att dessa processer och rutiner finns dokumenterade.

Kostnader 14 §

När det gäller kostnader som föranleds av föreslaget krav är storleken på kostnaderna beroende på vilken nivå av loggning som leverantören har idag samt leverantörens arbete med att åtgärda identifierade risker, se även avsnitt 4.1.2.

De administrativa engångskostnaderna kan avse kostnader för upprättande eller anpassningar av befintliga loggar, exempelvis loggning av fler uppgifter eller system. De administrativa kostnaderna kan även bestå av den eventuellt ytterligare dokumentation som leverantören behöver ta fram. I händelse av att leverantören behöver utöka eller på annat sätt förändra sin loggning eller sin dokumentation över sin loggning, uppskattar PTS att de administrativa engångskostnaderna uppgår till 20 000 kronor, givet en tidsåtgång om 40 timmar och en lönekostnad om 500 kronor/timme. En ytterligare administrativ engångskostnad kan gälla i det fall leverantören behöver kontrollera loggar vid misstanke om incident. PTS uppskattar att de administrativa engångskostnaderna för genomgång av loggar kan uppgå till 15 000 kronor, givet en tidsåtgång om 30 timmar och en lönekostnad om 500 kronor/timme.

De övriga kostnaderna kan exempelvis bestå av investering som kan komma att krävas efter riskbedömning är anskaffning av mjukvara, hårdvara eller licenser för loggning. Det finns många olika typer av logghanterings- och logganalystjänster som erbjuds på marknaden. Kostnaden för dessa tjänster grundar sig på olika affärsmodeller. Vissa tjänsteleverantörer baserar licenskostnaden per Gbyte lagrade data/uppgifter, andra på öppen källkod och kan därmed erbjuda andra priser. Prisuppgifter för loggning lämnas på offertbasis från loggningstillhandahållare, varför PTS inte har denna uppgift.

Kostnader för allmänt råd

Det föreslagna tillhörande allmänna rådet till 14 § förtydligar och ger vägledning kring aspekter av spårbarhet. Det allmänna rådet medför inga kostnader utöver de kostnader som följer av förslaget krav då det föreslagna allmänna rådet endast förtydligar bestämmelsen.

4.6 Åtgärder för att minimera verkningar av incidenter

4.6.1 Övervakning och incidenthantering 15 §

15 § Leverantören ska, i den utsträckning som följer av 6 §, vidta åtgärder för att säkerställa att inträffade incidenter upptäcks och avhjälps skyndsamt. Leverantören ska upprätta och tillämpa processer och rutiner för intern rapportering, analys och avhjälpande av en inträffad incident. Vid incidenthantering ska leverantören tillämpa processer och rutiner som utgår från etablerad standard på området. Processerna och rutinerna ska dokumenteras och hållas uppdaterade.

Allmänt råd om incidenthantering, 15 §

Leverantören bör använda övervakningssystem med anpassade larmnivåer för att kunna bedöma avvikelser i säkerheten i sina olika nätverk och informationssystem.

Leverantören bör ha beredskap dygnet runt för att kunna ta emot larm och initiera relevanta åtgärder skyndsamt vid händelse av en uppkommen incident.

En process för incidenthantering kan bl.a. omfatta bedömningskriterier för att avgöra vad som är en incident som ska hanteras, tillvägagångssätt och åtgärder för ett snabbt och effektivt avhjälpande av incidenten och en dokumenterad prioritetsordning för åtgärder som ska vidtas vid olika typer av incidenter.

Kravet innebär att leverantören, utifrån vad som framkommit i riskanalysen, ska vidta åtgärder för att upptäcka och avhjälpa incidenter skyndsamt samt tillämpa processer och rutiner för incidenthantering utifrån vad som framkommit i leverantörens genomförda riskbedömning. Vilka åtgärder som konkret ska vidtas framgår inte av föreskrifterna.

Syftet med kravet är att leverantören ska säkerställa att intern rapportering och utredning av incidenter sker så att skyndsamma åtgärder kan vidtas för att hantera uppkomna incidenter. Processerna för incidenthantering ska ta sin utgångspunkt i etablerad standard och ska vara dokumenterade. Exempel på etablerade standarder på området är ISO/IEC 27002 och ISO/IEC 27035.

Dokumenterade processer för att internt rapportera incidenter underlättar leverantörens arbete med att säkerställa att inträffade incidenter tas om hand på ett systematiskt och effektivt sätt samt minskar eventuella personberoenden.

Allmänna råd om incidenthantering

Det föreslagna tillhörande allmänna rådet till 15 § förtydligar och ger vägledning kring aspekter av övervakning och incidenthantering. Om en incident har inträffat bör det som regel medföra att säkerhetsåtgärderna skyndsamt ses över.

Kostnader 15 §

När det gäller kostnader som föranleds av föreslaget krav är storleken på kostnaderna beroende på vilken nivå av övervakning och incidenthantering som leverantören har idag samt leverantörens arbete med att åtgärda identifierade risker, se även avsnitt 4.1.2.

PTS bedömer att samtliga leverantörer har övervakning som genererar larm över åtminstone ett antal nätverk och informationssystem idag. Hur betungande kravet är för en enskild aktör är beroende av hur dennes befintliga övervakningssystem och upprättade larmnivåer samt incidenthanteringsprocesser ser ut idag. I händelse av att en leverantör har mindre utvecklade processer för incidenthantering på plats kan kravet medföra vissa kostnader för att exempelvis uppföra ytterligare övervakning för fler nätverk eller informationssystem, definiera ytterligare larmnivåer och bygga upp sin förmåga att hantera incidenter.

Administrativa engångskostnader som kravet kan komma att ge upphov till är eventuella anpassningar av befintliga dokumenterade processer och rutiner om skyndsam upptäckt och avhjälpande av inträffade incidenter, arbetstid för att komplettera leverantörens övervakning eller eventuella andra ytterligare behov av åtgärder när det gäller t.ex. skyndsam utredning och avhjälpning av inträffade incidenter.

I det fall leverantören behöver komplettera dokumentationen av sina befintliga processer och rutiner för övervakning och incidenthantering uppgår den administrativa engångskostnaden till 5 000 kronor, givet en tidsåtgång om 10 timmar och en lönekostnad om 500 kronor/timme.

PTS uppskattar att den årliga administrativa kostnaden uppgår till 2 500 kronor givet en tidsåtgång om fem timmar och en lönekostnad om 500 kronor/timme.

Övriga kostnader som kan uppkomma med anledning av föreslaget krav kan handla om att utbilda eller informera berörd personal om de eventuellt förändrade övervaknings- och incidenthanteringsrutinerna. I det fall leverantören behöver utbilda berörd personal om förändrade rutiner om incidenthantering, uppskattar PTS att den övriga kostnaden kan uppgå till 1000 – 2 000 kronor, givet att tidsåtgången är 1-2 timmar per utbildningstillfälle, två deltagare omfattas av utbildningen, och en lönekostnad är 500 kronor/timme.

Kostnader för allmänna råd

Det allmänna rådet avseende att ha beredskap dygnet runt för att kunna ta emot larm och initiera relevanta åtgärder skyndsamt kan medföra kostnader för de leverantörer som inte har denna beredskap idag.

De administrativa engångskostnaderna avser dokumentation av scheman för jourtjänstgöring, om detta behövs, och eventuella tillhörande dokument. PTS uppskattar att tidsåtgången för denna dokumentation uppgår till fyra timmar.

Den totala administrativa engångskostnaden uppgår till 2000 kronor, givet en lönekostnad om 500 kronor/timme.

De administrativa årliga kostnaderna avser eventuell revidering av dokumentationen, vilket PTS uppskattar till två timmar per år. Detta medför en årlig kostnad om 1000 kronor givet en lönekostnad om 500 kronor/timme.

Övriga kostnader som föranleds av det allmänna rådet bedöms uppgå till 3 200 kronor, givet att PTS uppskattar att det inträffar fyra incidenter som kräver skyndsam hantering under icke-kontorstid under ett år och tidsåtgången är en timme/incident och en lönekostnad om 800 kronor/timme.

4.6.2 Åtgärder för att undvika liknande incidenter i framtiden 16 §

16 § Leverantören ska, i den utsträckning som följer av 6 §, efter en incident vidta åtgärder för att undvika liknande incidenter i framtiden.

Allmänna råd
Lärdomar av inträffade incidenter, 16 §

Åtgärder för att dra lärdom av inträffade incidenter bör inkludera framtagande, tillämpning samt översyn av processer och rutiner. Processerna och rutinerna bör dokumenteras och hållas uppdaterade.

Kravet innebär att leverantören, utifrån vad som framkommit i leverantörens genomförda riskbedömning, ska vidta åtgärder för att undvika liknande incidenter i framtiden. Vilka åtgärder som konkret ska vidtas framgår inte av föreskrifterna.

Det är onödigt och kostsamt att redan inträffade incidenter, oavsett om de har drabbat leverantörens egna nätverk och informationssystem eller inte, inträffar på nytt. Syftet med kravet är att effektivisera incidenthanteringen och höja kvaliteten på säkerheten i nätverken och informationssystemen.

Allmänt råd om att dra lärdomar av inträffade incidenter

Enligt det till 16 § tillhörande allmänna rådet bör processerna och rutinerna även säkerställa att leverantören kan dra lärdomar från incidenterna i det framtida säkerhetsarbetet.

Kostnader 16 §

När det gäller kostnader som föranleds av föreslaget krav är storleken på kostnaderna beroende på i vilken utsträckning som leverantören idag vidtar åtgärder för att dra lärdom efter inträffade incidenter, se även avsnitt 4.1.2.

För det fall en leverantör har mindre ambitiösa processer för att dra lärdom av inträffade incidenter på plats kan kravet medföra vissa kostnader för att upprätta eller komplettera befintliga åtgärder.

Administrativa engångskostnader som kravet kan komma att ge upphov till är de eventuellt ytterligare organisatoriska åtgärder som leverantören behöver vidta utifrån utfallet i genomförd riskbedömning. I det fall en leverantör behöver revidera framtagna processer och rutiner för att dra lärdom efter inträffade incidenter kan det antas att givet att lönekostnaden är 500 kronor/timme och tidsåtgången för att revidera processer och rutinerna tar tre timmar uppgår kostnaden till 1 500 kronor.

I det fall ett möte om att dra lärdomar efter det att principiellt intressanta incidenter inträffat införs, med fem personer à 1,5 timme, och lönekostnaden uppgår till 500 kronor/timme, innebär det en administrativ kostnad om 3 750 kronor. PTS uppskattar att det sker i snitt tio principiellt viktiga incidenter per år, vilket medför en administrativ kostnad om 37 500 kronor.

I det fall leverantören inför en ny organisatorisk åtgärd som innebär att dokumentera samt tillgängliggöra dragna lärdomar på lämpligt sätt uppskattar kostnaden enligt följande. Tidsåtgången för att dokumentera och distribuera dragna lärdomar uppgår till 5 timmar med en lönekostnad om 500 kronor/timme, uppgår den administrativa kostnaden till 2 500 kronor. I det fall leverantören drabbas av tio incidenter som leverantören bedömer nödvändiga att sprida kunskap om på ett år uppgår den årliga administrativa kostnaden till 25 000 kronor.

Övriga kostnader som uppkommer med anledning av föreslaget krav kan handla om att leverantören behöver utbilda eller genomföra en informationsinsats om den förändrade processen.

I händelse av att leverantören behöver anordna en internutbildning om de förändrade processerna och rutinerna med anledning av föreslaget krav, uppskattar PTS de övriga kostnaderna till 2 000 kronor, givet fyra deltagare, en tidsåtgång för utbildningsinsatsen om en timme och en lönekostnad om 500 kronor/timme.

Kostnader för allmänt råd

Det föreslagna tillhörande allmänna rådet till 16 § förtydligar och ger vägledning kring aspekter av tillvaratagande av erfarenheter. Det allmänna rådet kan medföra kostnader för att ta fram processer och rutiner för det fall leverantören inte har sådana på plats. I händelse av att leverantören behöver se över och

komplettera sin process för att dra lärdom av inträffade incidenter samt komplettera dokumentationen över detsamma uppskattar PTS att de administrativa engångskostnaderna uppgår till 5 000 kronor givet en lönekostnad om 500 kronor/timme och en tidsåtgång för arbetet om tio timmar.

4.6.3 Kontinuitetsplanering 17-19 §§

17 § Leverantören ska identifiera och dokumentera de kritiska nätverk och informationssystem som krävs för att kunna upprätthålla kontinuiteten i tillhandahållandet av den samhällsviktiga tjänsten.

Leverantören ska analysera konsekvenserna för kontinuiteten i tillhandahållandet av den samhällsviktiga tjänsten som kan uppstå när de kritiska nätverken och informationssystemen helt eller delvis upphör att fungera (konsekvensanalys).

Konsekvensanalysen ska dokumenteras och hållas uppdaterad.

18 § Leverantören ska utifrån konsekvensanalysen i 17 § ta fram planer för att upprätthålla kontinuiteten i tillhandahållandet av den samhällsviktiga tjänsten även i händelse av omfattande incidenter (kontinuitetsplanering). Kontinuitetsplanerna ska åtminstone innehålla följande:

1. accepterad återställandetid,

2. när och hur alternativa arbetssätt ska användas för att upprätthålla kontinuiteten vid omfattande incidenter,

3. hur alternativa arbetssätt för att upprätthålla kontinuitet övas, samt

4. hur arbetet för att upprätthålla kontinuitet utvärderas och vid behov utvecklas.

Leverantören ska utgå från etablerad standard på området vid framtagande av kontinuitetsplanerna. Kontinuitetsplanerna ska dokumenteras och hållas uppdaterade.

19 § Leverantören ska tillämpa kontinuitetsplaner enligt 18 § i händelse av omfattande incidenter.

Allmänna råd

Tillämpning av kontinuitetsplaner, 18 §

Leverantören bör planera för att upprätthålla de kritiska nätverk och informationssystem som är absolut nödvändiga för den samhällsviktiga tjänstens kontinuitet även i de fall ordinarie linjeorganisation och incidenthantering inte klarar att upprätthålla kontinuiteten i tillhandahållandet av den samhällsviktiga tjänsten.

Kraven innebär att leverantören ska planera för att upprätthålla kontinuiteten i tillhandahållandet av den samhällsviktiga tjänsten i händelse av att kritiska nätverk eller informationssystem helt eller delvis upphör att fungera.

Syftet med kraven är att begränsa konsekvenserna i händelse av omfattande incidenter i kritiska nätverk eller informationssystem. Analyserna ger ett nödvändigt beslutsunderlag för att leverantören ska kunna ta fram de relevanta

kontinuitetsplaner som behövs för att säkerställa att verksamheter har en beredskap för att hantera det oväntade och oförutsedda. Genom kontinuitetsplaneringen säkerställs att det finns resurser, befogenheter och dokumenterade tillvägagångssätt över hur organisationen ska agera vid händelser som slår ut kritiska nätverk och informationssystem. Planerna kan t.ex. omfatta definierade tillvägagångssätt och återställandeåtgärder, prioritetsordningar, processer för att säkerställa att extra resurser kan avsättas när det är nödvändigt, samt säkerställande av att det finns en tydlig organisation för utförande av beslutade åtgärder och uppgifter om vem som är ansvarig för att olika åtgärder vidtas samt former för vidarerapportering inom verksamheten. På sikt bedöms kravet kunna leda till en ökad kontinuitet hos den samhällsviktiga tjänsten, vilket bedöms innebära lägre kostnader för leverantörerna med anledning av incidenter.

Leverantören ska ta sin utgångspunkt i etablerad standard vid framtagande av kontinuitetsplanerna. Detta säkerställer en enhetlig tillämpning som håller över tid. Exempel på etablerade standarder är ISO/IEC 27002 och ISO/IEC 22301.

Kravet på dokumentation av konsekvensanalys och kontinuitetsplaner utgör en förutsättning för en systematisk uppföljning av säkerhetsarbetet och kontroll av vilka bedömningar som gjorts inom ramen för kontinuitetsplaneringen.

Allmänt råd om kontinuitetsplanering

Det tillhörande allmänna rådet till de föreslagna bestämmelserna om kontinuitetsplanering förtydligar och ger vägledning kring aspekter vid genomförande av kontinuitetsplanering.

Kostnader 17-19 §§

Krav på kontinuitetsplanering framgår redan av NIS-lagen och MSB:s informationssäkerhetsföreskrifter. Mot denna bakgrund begränsas kostnaderna av föreslagna krav om kontinuitetsplanering. Det är dock PTS bedömning att många leverantörer idag inte fullt ut arbetar med kontinuitetsplanering i enlighet med föreslagna krav eller endast i begränsad omfattning. Föreslagna krav medför därför i viss utsträckning kostnader för leverantörerna.

De administrativa engångskostnaderna avser kostnader för de eventuellt ytterligare mallar för dokumentation av kritiska nätverk och informationssystem, konsekvensanalys och kontinuitetsplanering som behöver upprättas eller kompletteras. Ytterligare administrativa engångskostnader utgörs av identifiering av kritiska nätverk och informationssystem för upprätthållande av kontinuiteten av den samhällsviktiga tjänsten, genomförande och dokumentation av konsekvensanalyser.

I det fallet leverantören behöver komplettera sin kontinuitetsplanering i enlighet med föreslaget krav uppskattar PTS att de administrativa engångskostnaderna för identifiering och dokumentation av kritiska nätverk och informationssystem

uppgår till 12 500 kronor, givet en lönekostnad om 500 kronor/timme samt en tidsåtgång för arbetet om 25 timmar.

De administrativa årliga kostnaderna avser fortsatt identifiering av kritiska nätverk och informationssystem, genomförande av uppdateringar av konsekvensanalyser och eventuell fortsatt dokumentation av genomförda analyser och planer. PTS uppskattar att de administrativa årliga kostnaderna för att hålla dokumentationen för kontinuitetsplanering uppdaterad uppgår till 4000 kronor/år, givet att tidsåtgången för arbetet tar åtta timmar och en lönekostnad om 500 kronor/timme.

PTS bedömer att de övriga kostnaderna som är förknippade med föreslagna krav är hänförliga till personalkostnader, såsom kostnader för eventuell utbildning av personal avseende konsekvensanalysarbete. Dessa kostnader bedöms dock inte vara särskilt omfattande eftersom PTS bedömer att den personal hos leverantören som arbetar med dessa frågor i de flesta fall är förtrogna med sådant analysarbete. Kommande år bedöms att ny personal behöver utbildas. De kostnader som skulle kunna uppstå kan röra sig om att anordna ett informationsmöte eller en internutbildning. Det nu föreslagna kravet kan medföra en extra tidsåtgång om 1 – 2 timmar per deltagare. Om den interna utbildningsinsatsen omfattar 4 deltagare med en lönekostnad om 500 kronor/timme uppgår den övriga kostnaden till 2 000 - 8 000 kr.

Kostnader för allmänt råd

Det tillhörande allmänna rådet till de föreslagna bestämmelserna om kontinuitetsplanering förtydligar och ger vägledning kring aspekter vid genomförande av kontinuitetsplanering. Det allmänna rådet medför inga kostnader utöver de kostnader som följer av förslagna krav då det föreslagna allmänna rådet endast förtydligar bestämmelserna.

4.7 Påverkan på konkurrensförhållandena för företagen

De företag som berörs av regleringen verkar på en konkurrensutsatt marknad och är de största på marknaden när det gäller tillhandahållande av DNS-tjänster - de med flest domännamn anslutna till sin namnservertjänst samt de med flest användare av sin namnservertjänst. Företag, organisationer och konsumenter som är i behov av en leverantör av en namnservertjänst, väljer fritt bland dem som finns på marknaden.

I och med att PTS ställer upp krav för leverantörerna finns det risk för att förutsättningar för hur marknaden fungerar förändras och därmed villkoren för konkurrensen. MSB:s informationssäkerhetsföreskrifter gäller sedan den 1 november 2018 och reglerar ett systematiskt och riskbaserat informationssäkerhetsarbete som omfattar arbetet med riskanalyser, säkerhetsåtgärder, incidenthantering och kontinuitetsplanering. Mot bakgrund av att leverantörerna därmed redan idag är skyldiga att bedriva ett systematiskt riskbaserat informationssäkerhetsarbete medför de nu föreslagna föreskrifterna

endast kompletterande och förtydligande krav. Dessutom är det leverantörernas genomförda riskanalys som ligger till grund för val av säkerhetsåtgärder. Utöver detta kan det konstateras att leverantörerna av dessa samhällsviktiga tjänster sedan flera år bedriver ett säkerhetsarbete, har upparbetade organisatoriska förmågor inom säkerhet och får antas ha upprättat en robust infrastruktur. Mot denna bakgrund bedömer PTS att leverantörerna redan idag har ett flertal (tekniska) säkerhetsåtgärder på plats.

Därmed bedömer PTS att de föreskrifter som nu föreslås kan antas påverka de företag som verkar på marknaden i mycket liten utsträckning. PTS gör sammantaget bedömningen att konkurrensförhållandena på marknaden i mycket liten utsträckning torde påverkas av den föreslagna regleringen.

4.8 Föreskrifternas effekter för kommuner och regioner

Inga effekter förutses.

4.9 Konsekvenser för konsumenter

Konsumenter och hushåll kan förväntas påverkas av de föreslagna föreskrifterna genom att föreskrifterna bidrar till en ökad tillförlitlighet och tillgänglighet till tjänster som förlitar sig på domännamn, exempelvis webbplatser, e-tjänster och onlineförsäljning. Detta bidrar i sin tur till konsumenternas tillit till webbaserade tjänster, som kan leda till att samhällsutveckling och ekonomisk tillväxt gynnas.

5 Övrigt

5.1 Regleringens överensstämmelse med de skyldigheter som följer av Sveriges anslutning till EU

Nu aktuella föreskrifter har utformats i enlighet med bestämmelserna i 12-14 §§ NIS-lagen. Bestämmelserna 13-14 §§ NIS-lagen genomför artikel 14 punkten 1 och 2 NIS-direktivet. Bestämmelsen i 12 § NIS-lagen är nationell, men återspeglar kravet i artikel 14 NIS-direktivet så att en nivå på säkerheten i nätverk och informationssystem ska vara lämplig i förhållande till risken.

De föreslagna föreskrifterna ger ett yttre ramverk för riskbedömning, genomförande av säkerhetsåtgärder samt kontinuitetsplanering. Förslaget till föreskrifter förtydligar lämpliga åtgärder som leverantörer av samhällsviktiga tjänster inom sektorn digital infrastruktur efter genomförd riskanalys och beroende på utfallet av riskanalysen ska vidta enligt 12-14 §§ NIS-lagen.

PTS bedömer att förslaget till nya föreskrifter är i överensstämmelse med NIS-direktivet.

5.2 Behovet av särskilda hänsyn till små företag

PTS har beaktat frågan om särskilda hänsyn behöver tas till små företag vid reglernas utformning. Kraven fastställer vad som ska uppnås, inte hur. De föreslagna föreskrifterna lämnar därmed ett stort utrymme för leverantörerna att göra egna bedömningar av behovet av åtgärder.

Bland de som berörs av föreskrifterna uppskattar PTS att det finns allt från företag med en årsomsättning på 26 miljoner kronor till företag med en årlig omsättning på ca 182 miljoner kronor. PTS bedömer sammanfattningsvis att kostnaderna för att uppfylla bestämmelserna i föreskrifterna är rimliga i förhållande till behovet och nyttan av säkerhet i nätverk och informationssystem. PTS bedömer att någon särskild hänsyn inte behöver tas till små företag vid reglernas utformning.

5.3 Tidpunkten för ikraftträdande och behovet av speciella informationsinsatser

NIS-lagen har varit i kraft sedan den 1 augusti 2018 och MSB:s informationssäkerhetsföreskrifter har varit i kraft sedan den 1 november 2018. De nu föreslagna föreskrifterna kompletterar genomförandet av NIS-direktivet och bör därför träda i kraft så snart som möjligt. Genom att de föreslagna föreskrifterna förtydligar NIS-lagen möjliggörs en enhetlig tillämpning av reglerna. Mot denna bakgrund föreslår PTS att föreskrifterna träder i kraft senast den 1 december 2020.

Förutom att samtliga berörda företag får information om de föreslagna föreskrifterna i samband med att föreskriftsförslaget remitteras kommer PTS att ta fram allmän information med anledning av de nya föreskrifterna, som kommer att publiceras på PTS webbplats.

6 Avslutning

6.1 Underrättelse för anmälan till Europeiska kommissionen

I 6 § förordningen (1994:2029) om tekniska regler framgår att en myndighet som avser fatta beslut om en teknisk regel i god tid ska underrätta Kommerskollegium om det förslag som den har utarbetat. Bestämmelserna i förordningen ansluter till Sveriges internationella förpliktelser enligt bl.a. Europaparlamentets och rådets direktiv (EU) 2015/1535 om ett informationsförfarande beträffande tekniska standarder och föreskrifter och beträffande föreskrifter för informationssamhällets tjänster.

Enligt PTS bedömning är nu föreslagna föreskrifter inte att se som sådana tekniska regler som ska underrättas enligt nämnda förordning. Någon underrättelse till Kommerskollegium behöver således inte göras.

6.2 Kontaktuppgifter

Kontaktpersoner för sakfrågor:

Erika Hersaeus, PTS avdelning för säker kommunikation:

Erika.Hersaeus@pts.se

Isabelle Westerlund, PTS avdelning för säker kommunikation:

Isabelle.Westerlund@pts.se

Kontaktperson för juridiska frågor:

Cecilia Östrand, PTS rättsavdelning:

Cecilia.Ostrand@pts.se