Post- och telestyrelsens författningssamling

ISSN 1400-187X

Post- och telestyrelsens föreskrifter om säkerhetsåtgärder för samhällsviktiga tjänster inom sektorn digital infrastruktur;

PTSFSÅR:NR

Utkom från trycket den välj datum

beslutade den välj datum.

Post- och telestyrelsen föreskriver[1] följande med stöd av 8 § förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Tillämpningsområde

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.

Ord och uttryck

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).

Riskanalys och riskbedömning

4 § Leverantören ska identifiera samtliga nätverk och informationssystem som används för att tillhandahålla den samhällsviktiga tjänsten.

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 säkerheten i 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 säkerheten i nätverk och informationssystem inträffar,

[1] Se Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska standarder och föreskrifter och beträffande föreskrifter för informationssamhällets tjänster.

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

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

Den valda riskanalysmetoden ska utgå från etablerad standard.

Allmänna råd

Gruppering av nätverk och informationssystem, 4 §

Leverantören kan välja att kategorisera likvärdiga nätverk eller informationssystem som används för att tillhandahålla den samhällsviktiga tjänsten 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. Ett annat hot som också bör analyseras är eventuell brist på utrustning och reservdelar till kritiska nätverk och informationssystem.

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 förutbestämda nivåer exempelvis mycket sällsynt, tämligen sällsynt, regelbundet och ofta. Konsekvensbedömningar på säkerheten i nätverk och informationssystem kan delas in i olika förutbestämda nivåer såsom försumbar, lindrig, måttlig, allvarlig och katastrofal. Nivåerna bör vara enhetliga och jämförbara över tid.

För att tillse kvalificerade bedömningar sker bör leverantören 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 beskrivning av vald riskanalysmetod samt leverantörens ingående kriterier för nivåer av sannolikhet och konsekvens,

4. redogörelser av skälen till bedömning enligt 4 § andra stycket 2 - 4,

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

Åtgärder och åtgärdsplan

6 § Leverantören ska bedöma om riskerna ska elimineras, reduceras eller accepteras utifrån genomförd riskbedömning i 4 §. Om leverantören behöver eliminera eller reducera identifierade risker 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 utifrån genomförd riskbedömning i 4 §. Samtliga åtgärder ska vidtas på en nivå som är proportionerlig i förhållande till den föreliggande risken.

Redogörelser av skälen för bedömning av om riskerna ska elimineras, reduceras eller accepteras ska dokumenteras.

Allmänna råd
Eliminering, reducering eller acceptans av risker, 6 §

Leverantören bör beakta den senaste tekniska utvecklingen för att säkerställa en nivå på säkerheten i nätverk och informationssystem som är lämplig i förhållande till den föreliggande risken.

Leverantören bör endast acceptera risker om riskbedömningen i det aktuella fallet påvisar att säkerheten i den samhällsviktiga tjänsten kan upprätthållas.

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. ansvarig befattning i organisationen för att vidta åtgärden,
7. när åtgärden ska vara genomförd, samt
8. när åtgärden har vidtagits.

Leverantören ska följa upp och utvärdera vidtagna åtgärder.

Fysiska och logiska skydd

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 privata krypteringsnycklar i det fall asymmetrisk kryptering används.

Säker programvaruhantering

9 § 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, 10 §

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.

Fysisk och logisk behörighets- och åtkomsthantering

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 de personer eller de specifika processer i 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 de specifika processer i system som är behöriga till nätverk och informationssystem.

Flerfaktorsautentisering bör användas vid åtkomst till informationssystem från externa nätverk.

Hantering av planerade tekniska och organisatoriska förändringar

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.

Säkerställande av kompetens och personella resurser

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.

Spårbarhet

14 § Leverantören ska, i den utsträckning som följer av 6 §, säkerställa spårbarhet genom att 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 och 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 följa upp 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 två 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.

Systemhändelser, 14 §

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

Uppgifter som är konfidentiella, 14 §

Med ”sådana uppgifter som är konfidentiella” avses exempelvis autentiseringsuppgifter och privata krypteringsnycklar i det fall asymmetrisk kryptering används.

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.

Åtgärder för att minimera verkningar av incidenter

Övervakning, larm och incidenthantering

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.

Allmänna råd
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.

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.

Kontinuitetsplanering

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.

Allmänna råd
Konsekvensanalys 17 §

Leverantören bör analysera konsekvenserna av eventuella brister på tillgång till sådan utrustning eller sådana reservdelar som behövs för att kritiska nätverk och informationssystem ska kunna upprätthålla kontinuiteten i den samhällsviktiga tjänsten.

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, 19 §

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.

Dessa föreskrifter träder i kraft den välj datum.

På Post- och telestyrelsens vägnar

NAMN

Namn