Transportstyrelsens författningssamling

TRANSPORT STYRELSEN

TSFS 20[YY]:[XX]

Utkom från trycket
den [DATUM ÅR]

Transportstyrelsens föreskrifter och allmänna råd om säkerhetsåtgärder för leverantörer av samhällsviktiga tjänster inom transportsektorn;

beslutade den [DATUM ÅR].

Transportstyrelsen föreskriver följande med stöd av 8 § förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster och beslutar följande allmänna råd.

Inledande bestämmelser

Tillämpningsområde

1 § Dessa förskrifter gäller för leverantörer som omfattas av lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och som tillhandahåller sådana samhällsviktiga tjänster som identifierats inom transportområdet i enlighet med 3 § förordning (2018:1175) om samhällsviktiga och digitala tjänster.

2 § Dessa föreskrifter innehåller kompletterande bestämmelser till de säkerhetsåtgärder som leverantörer ska vidta enligt 12, 13 och 14 §§ lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

3 § Leverantörens skyldigheter enligt dessa föreskrifter gäller även när leverantören utkontrakterar hanteringen av nätverk och informationssystem.

Uttryck i föreskrifterna

4 § Ord och uttryck som används i dessa föreskrifter har samma innebörd som i lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Definitioner

5 § I dessa föreskrifter används följande termer och definitioner.

arbetssätt	organisationens styrande dokument som konkretiserar interna regler, exempelvis anvisningar eller instruktioner

autentisering	verifiering av uppgiven identitet
drifts-godkännande	beslut om att ett nätverk eller informationssystem kan godkännas för drift med användning av en beskriven uppsättning säkerhetsfunktioner och skyddsåtgärder
härdning	innebär att de operativsystem, inbyggda programvaror, nätverkskomponenter, databaser och andra applikationer som ingår i ett informationssystem konfigureras på ett så säkert sätt som möjligt
interna regler	organisationens övergripande styrande dokument, exempelvis policy eller riktlinjer
intrångsdetekteringssystem (IDS)	verktyg (enhet eller programvara) som används för att automatiskt upptäcka dataintrång eller dataintrångsförsök
segmentering	uppdelning av IT-miljö i olika nätverkssegment med fysisk eller logisk separation

Säkerhetsåtgärder

Inventering

6 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för inventering av nätverk och informationssystem, i syfte att identifiera vilka nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten.

Förteckning av informationstillgångar

7 § Leverantören ska utifrån den inventering som genomförts enligt 6 § upprätta förteckning över informationstillgångar. Förteckningen ska innehålla de informationstillgångar som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten. Förteckningen ska hållas uppdaterad.

Allmänna råd

Exempel på informationstillgångar är

1. information (data, dokument etc.),

2. program (applikationer, operativsystem etc.),

3. tjänster (kommunikationstjänster, abonnemang etc.),

4. fysiska tillgångar (datorer, datamedier, lokaler, lokala nätverk etc.), och

5. befattningar, roller och funktioner.

Omvärldsbevakning

8 § Leverantören ska bedriva omvärldsbevakning för att identifiera hot mot och sårbarheter i de nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten.

Riskanalys

9 § Av 12 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster framgår att leverantören ska genomföra en riskanalys. I riskanalysen ska leverantören beakta den förteckning av informationstillgångar som upprättats, resultatet av den omvärldsanalys som genomförts och incidenter som inträffat.

Åtgärdsplan

10 § Av 12 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster framgår att riskanalysen ska innehålla en åtgärdsplan. I åtgärdsplanen ska det framgå vilka åtgärder som motverkar vilka risker, vilka nätverk och informationssystem som åtgärderna avser, vilka tidigare åtgärder som genomförts, hur risknivån förväntas förändras och när åtgärderna senast ska vara genomförda.

Uppföljning

11 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för uppföljning och analys av vidtagna säkerhetsåtgärders effektivitet.

Driftsgodkännande

12 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för driftsgodkännande av de nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten. Av de dokumenterade reglerna ska det framgå vilka kriterier som ska användas för att godkänna hård- och mjukvara innan installation eller användning.

Ändringshantering, uppgradering och uppdatering

13 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för de planerade tekniska eller organisatoriska förändringar som kan påverka de nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten. De interna reglerna ska innehålla krav på att

1. mjukvara, i de system där det är möjligt, löpande uppdateras till senaste version,
2. hård- och mjukvara som inte längre uppdateras eller stöds av leverantören, om möjligt, byts ut eller uppgraderas.

Säkerhetstester och revision

14 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för säkerhetstester och granskningar av nätverk och informationssystem. Säkerhetstester och granskningar ska möjliggöra identifiering av sårbarheter som kan påverka kontinuiteten i den samhällsviktiga tjänsten.

Utbildningsplan

15 § Leverantören ska ta fram, fastställa och tillämpa en utbildningsplan för de befattningar, roller och funktioner som har ansvarsuppgifter kopplade till de nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten. Planen ska innefatta informationssäkerhetshöjande utbildningar, repetitionsutbildningar, övningar och beskrivningar av utbildningsinsatsers målgrupper, mål och syften. Genomförda utbildningar, repetitionsutbildningar och övningar ska dokumenteras.

Härdning

16 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för inaktivering av oanvända tjänster och protokoll (härdning) i de nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten.

Allmänna råd

Leverantörens arbetssätt för härdning bör följa produktleverantörens rekommendationer och etablerade standarder för härdning.

Segmentering

17 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för segmentering av de nätverk som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten.

Allmänna råd

Nätverket bör segmenteras utifrån informationssystemens funktion och värdet på informationen som hanteras i dem.

Filtrering

18 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för filtrering av nätverkstrafik, så att endast nödvändiga dataflöden förekommer mellan de nätverkssegment som behövs för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten.

Kryptering

19 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för att hantera behovet av kryptering, i syfte att skydda information mot obehörig åtkomst och obehörig förändring vid överföring och lagring.

Identiteter

20 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för upprättandet av unika identiteter för användare, systemadministratörer, och automatiserade processer. Leverantören ska löpande föra förteckning över tilldelade identiteter. Identiteter ska avaktiveras när de inte längre används eller behövs.

Behörigheter

21 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för hantering av behörigheter. De interna reglerna ska beskriva när behörigheter ska följas upp och på vilka grunder de tilldelas, ändras, och återkallas. Leverantören ska löpande föra förteckning över tilldelade behörigheter. En användare eller automatiserad process ska endast tilldelas den behörighet som är nödvändigt för arbetsuppgiften.

Systemadministrativa behörigheter

22 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för hantering av systemadministrativa behörigheter. De interna reglerna ska beskriva när systemadministrativa behörigheter ska följas upp och på vilka grunder de tilldelas, ändras, och återkallas. Systemadministrativa behörigheter ska endast användas för systemadministrativa uppgifter. Tilldelning av systemadministrativa behörigheter ska vara restriktiv och endast tilldelas om det är nödvändigt för arbetsuppgiften. Leverantören ska löpande föra förteckning över tilldelade systemadministrativa behörigheter.

Systemadministrativt arbete

23 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för systemadministrativt arbete i nätverk och informationssystem. Av det dokumenterade arbetssättet ska det framgå hur hårdvaru- och mjukvarutillgångar som används för systemadministrativa uppgifter underhålls och konfigureras.

Autentisering

24 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för autentisering av identiteter enligt 20 §. Vid

fjärr- eller systemadministrativ åtkomst till de nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten, ska autentiseringen baseras på flera faktorer (flerfaktorsautentisering).

Skydd av utrustning

25 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för skydd av utrustning mot skador av och obehörig fysisk åtkomst till utrustning för de nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten.

Allmänna råd

Leverantören bör skydda utrustning för de nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i tillhandahållandet av den samhällsviktiga tjänsten, genom att

1. placera centrala servrar och central nätverksutrustning i särskilda IT-utrymmen,

2. restriktivt tilldela behörighet till att tillträda särskilda IT-utrymmen,

3. identifiera och hantera behovet av övervakning och larm i särskilda IT-utrymmen,

4. på individnivå registrera tillträde till särskilda IT-utrymmen och spara dokumentationen under fastställd bevarandetid, och

5. ha interna regler för hur mobil utrustning ska skyddas.

Detektering av dataintrång

26 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för identifiering av dataintrång. Där det är lämpligt ska leverantören anskaffa och använda intrångsdetekteringssystem (IDS) för de nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten.

Skydd mot skadlig kod

27 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för skydd mot skadlig kod i de nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten. Där mjukvara för skydd mot skadlig kod inte är lämplig eller tillgänglig ska andra åtgärder vidtas för att uppnå ett motsvarande skydd.

Säkerhetsloggning

28 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för att säkerställa spårbarhet i säkerhets-

relaterade händelser avseende de nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten. Av arbetssättet ska det framgå hur säkerhetsloggar skyddas mot avsiktlig eller oavsiktlig förändring, förlust och radering.

Allmänna råd

För att skapa en jämförbarhet bör leverantören se till att samtliga loggkällor använder gemensam tid.

Logganalys

29 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för logganalys, i syfte att upptäcka och hantera incidenter och avvikelser som kan påverka kontinuiteten i den samhällsviktiga tjänsten.

Återställningsförmåga

30 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för återställningsförmåga i händelse av en incident i de nätverk och informationssystem som används för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten. Interna regler och arbetssätt ska tydliggöra hur återställning av de informationstillgångar som upprättats enligt 7 § omhändertas i syfte att återställa kontinuiteten i den samhällsviktiga tjänsten.

Organisation och hantering av kris vid incidenter

31 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt gällande organisation och hantering av kriser som kan uppstå till följd av incidenter i de nätverk och informationssystem som används för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten.

Undantag

32 § Transportstyrelsen får medge undantag från dessa föreskrifter.

Denna författning träder i kraft den 1 januari 2022.

På Transportstyrelsens vägnar

JONAS BJELFVENSTAM

Fredrik Carlsson
(Sjö- och luftfart)

Utgivare: Kristina Nilsson, Transportstyrelsen, Norrköping ISSN 2000-1975