Statens energimyndighets författningssamling

Utgivare: Rikard Janson (chefsjurist)
ISSN 1650-7703

Statens energimyndighets föreskrifter och allmänna råd om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn

STEMFS 2021:3

Utkom från trycket den 3 februari 2021

beslutade den 20 januari 2021

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

1 kap. Inledande bestämmelser och definitioner

Tillämpningsområde

1 § I dessa föreskrifter finns bestämmelser för leverantörer av samhällsviktiga tjänster inom energisektorn om riskanalys enligt 12 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster samt om säkerhetsåtgärder enligt 13 och 14 §§ samma lag.

2 § Dessa föreskrifter avser en leverantörs nätverk och informationssystem som leverantören använder för att tillhandahålla samhällsviktiga tjänster.

För att identifiera vilka nätverk och informationssystem som leverantören använder för att tillhandahålla samhällsviktiga tjänster ska leverantören analysera sina nätverk och informationssystem. Om leverantören anlitar underleverantör för att stödja tillhandahållandet av de samhällsviktiga tjänsterna ska dessa nätverk och informationssystem omfattas av leverantörens analys.

Leverantören ska dokumentera den analysmetod som används enligt andra stycket liksom resultatet av analysen.

Definitioner

3 § Begrepp och uttryck i dessa föreskrifter har samma innebörd som i lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Dessutom betyder

leverantör: leverantör av tjänster rörande el, olja eller gasförsörjning enligt 3 kap. 1–3 §§ Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:7) om anmälan och identifiering av leverantörer av samhällsviktiga tjänster,

IT (från engelskans ”Information Technology”): nätverk och informationssystem med funktioner för administrativt bruk, utan funktioner att hantera verksamhetens cyberfysiska processer,

OT (från engelskans ”Operational Technology”): industriella informationssystem med huvudsaklig funktion att styra och övervaka en fysisk process,

informationssäkerhetskrav: funktionella krav på säkerhetsåtgärder i nätverk och informationssystem,

informationssystem: applikationer, tjänster eller andra komponenter som hanterar information.

2 kap. Riskanalys

1 § Enligt 12 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster ska leverantörer göra en riskanalys som ska ligga till grund för val av säkerhetsåtgärder enligt 13 och 14 §§ samma lag. Riskanalysen ska omfatta de nätverk och informationssystem som identifierats genom den analysen som utförts enligt 1 kap. 2 §.

De risker som leverantören har identifierat i riskanalysen ska värderas utifrån riskernas sannolikhet och konsekvens, varvid varje risk ska tilldelas ett riskvärde.

Leverantören ska även bedöma hur de identifierade riskerna kan påverka leveransen av den samhällsviktiga tjänsten.

3 kap. Informationssäkerhetskrav

1 § Utöver att hantera de risker som identifieras i riskanalysen enligt 2 kap. 1 § ska leverantören uppfylla de informationssäkerhetskrav som anges i 2 – 5 §§, varvid leverantören ska

1. dokumentera de processer och metoder som används för att uppfylla informationssäkerhetskraven, samt
2. utföra loggning i syfte att möjliggöra upptäckt, larm och spårning av transaktioner och händelser.

2 § Leverantören ska upprätta en systemförteckning över sin IT och OT genom att

1. kartlägga och analysera de IT- och OT-tjänster samt nätverk och informationssystem som används vid leverantörens tillhandahållande av samhällsviktiga tjänster samt hur dessa kommunicerar med och är beroende av varandra,

2. inventera vilka hårdvaror som används i leverantörens IT och OT,
3. inventera vilka mjukvaror som används i leverantörens IT och OT,
4. identifiera vilka interna och externa nätverk och informationssystem liksom vilka hårdvaror och mjukvaror som är mest kritiska för leverantörens tillhandahållande av samhällsviktiga tjänster, samt
5. upprätta en nätverkskarta avseende leverantörens IT och OT.

Systemförteckningen ska hållas uppdaterad.

3 § Leverantören ska skydda sina nätverk och informationssystem genom att

1. segmentera sitt nätverk och filtrera trafiken mellan olika nätverkssegment,
2. minimera användandet av administrationsrättigheter,
3. installera säkerhetsuppdateringar enligt vedertagna metoder,
4. använda proportionella autentiseringsmetoder,
5. om möjligt använda antivirusprogram på enheter som är uppkopplade mot IT och OT,
6. begränsa fysisk tillgång till IT och OT, samt
7. fastställa och upprätthålla regler och metoder för fjärråtkomst till leverantörens nätverk och informationssystem.

4 § Leverantören ska arbeta för att förebygga incidenter genom att

1. härda informationssystem innan de börjar användas, i den mån det inte medför nya risker,
2. hantera förändringar i nätverk och informationssystem med metoder som minimerar risk för störningar eller förändringar i IT:s och OT:s informationssäkerhet, samt
3. hantera informationssystem som har upphört att användas för att säkerställa att känslig information inte avslöjas.

5 § Leverantören ska minimera verkningar av incidenter genom att

1. säkerhetskopiera applikationer och information från de delar av IT och OT som är kritiska för tillhandahållande av samhällsviktiga tjänster,
2. regelbundet testa återställning av säkerhetskopior, samt
3. säkerställa att nätverk och informationssystem är så redundanta som möjligt utifrån deras väsentlighet för tillhandahållande av den samhällsviktiga tjänsten och utifrån tekniska förutsättningar.

4 kap. Säkerhetsåtgärder

1 § Leverantören ska införa säkerhetsåtgärder dels för att hantera risker som identifierats enligt 2 kap. 1 §, dels för att uppfylla informationssäkerhetskrav enligt 3 kap. En säkerhetsåtgärd ska antingen sänka ett riskvärde eller uppfylla ett informationssäkerhetskrav.

2 § Enligt 12 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster ska leverantören göra en riskanalys som ska ligga till grund för val av säkerhetsåtgärder. I riskanalysen ska det ingå en åtgärdsplan. Åtgärdsplanen ska innehålla följande information avseende varje säkerhetsåtgärd som ingår i planen:

1. vilken risk säkerhetsåtgärden påverkar,
2. vilket nätverk eller informationssystem som säkerhetsåtgärden ska införas inom,
3. person eller funktion hos leverantören som ansvarar för säkerhetsåtgärden,
4. planerad tidsram för införande av säkerhetsåtgärden,
5. säkerhetsåtgärdens påverkan på riskens sannolikhet eller konsekvens enligt den värdering som gjorts enligt 2 kap. 1 §, samt
6. riskvärde efter säkerhetsåtgärdens införande.

3 § Enligt 14 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster ska leverantören vidta åtgärder för att förebygga och minimera verkningar av incidenter som påverkar nätverk och informationssystem som denne använder för att tillhandahålla den samhällsviktiga tjänsten. Inför införandet av åtgärder för att uppfylla informationssäkerhetskrav enligt 3 kap. ska leverantören ange:

1. vilket nätverk eller informationssystem som säkerhetsåtgärden ska utföras inom,
2. person eller funktion hos leverantören som ansvarar för säkerhetsåtgärden, samt
3. planerad tidsram för genomförande av säkerhetsåtgärden.

4 § Genomförandet av säkerhetsåtgärder ska prioriteras med beaktande av leverantörens riskvärdering enligt 2 kap. 1 § samt med beaktande av de ekonomiska och tidsmässiga resurser som vidtagandet av säkerhetsåtgärderna kan kräva.

5 kap. Undantag

1 § När särskilda skäl föreligger får Statens energimyndighet medge undantag från dessa föreskrifter.

Ikraftträdande

Dessa föreskrifter träder i kraft den 1 mars 2021.

På Statens energimyndighets vägnar

Robert Andrén

Göran Smedbäck

Allmänna råd till Statens energimyndighets föreskrifter om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn

Allmänna råd till 1 kap. om inledande bestämmelser och definitioner

1 §

Utöver Statens energimyndighets föreskrifter om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn finns Myndigheten för samhällsskydd och beredskaps (MSB) föreskrifter om:

- anmälan och identifiering av leverantörer av samhällsviktiga tjänster, MSBFS 2018:7,
- informationssäkerhet för leverantörer av samhällsviktiga tjänster, MSBFS 2018:8,
- rapportering av incidenter för leverantörer av samhällsviktiga tjänster, MSBFS 2018:9 samt,
- frivillig rapportering av incidenter i tjänster som är viktiga för samhällets funktionalitet, MSBFS 2018:11.

2 §

Vid fastställandet av vilka nätverk och informationssystem som ingår i leverantörens tillhandahållande av samhällsviktiga tjänster, och vad som därmed omfattas av leverantörens riskanalys, kan leverantören använda den kartläggning som ska utföras enligt 3 kap. 2 § punkt 1 och 4 denna föreskrift.

I analysen bör leverantören ta ställning till vilka delar av leverantörens nätverk och informationssystem som behövs för att kunna upprätthålla kontinuerligt tillhandahållande av samhällsviktiga tjänster, samt vilka delar av nätverket och informationssystemet som kan påverka tillhandahållandet om de inte fungerar på grund av bristande säkerhet.

I analysen bör leverantören även ta ställning till vilka applikationer och verktyg som krävs för att åtgärda krav från tidigare riskanalyser och informationssäkerhetskrav enligt 3 kap.

3 §

I begreppet ”IT” ingår bland annat e-post, delade filytor och applikationer för personaladministration, ekonomi, försäljning och produktivitet. Begreppet IT kallas ibland ”Kontors-IT”. Även nätverk som innefattar dessa informationssystem omfattas av i begreppet IT.

I begreppet ”OT” ingår bland annat det som kallas ICS (Industrial Control Systems), SCADA (Supervisory Control And Data Acquisition). Även nätverk som innefattar dessa informationssystem omfattas av begreppet OT.

Allmänna råd till 2 kap. om riskanalys

1 §

I samband med utförandet av riskanalysen kan leverantören ta i beaktande hur befintliga säkerhetsåtgärder påverkar de identifierade riskernas sannolikhet eller konsekvens.

I samband med utförandet av riskanalysen bör leverantören ta ställning till egenskaper och förutsättningar inom OT som kan behöva beaktas särskilt såsom följande.

1. Realtidsfunktionalitet är ofta en förutsättning för tillhandahållande av samhällsviktiga tjänster. Även en mycket kort störning kan få stora konsekvenser.
2. En mindre störning i OT kan få följdverkningar och innebära stor påverkan på omkringliggande informationssystem.
3. OT kan vara föråldrat på så sätt att det inte är avsett att vara uppkopplat enligt nuvarande användning. Detta kan medföra särskild sårbarhet i leverantörens nätverk och informationssystem.

Leverantörens bedömning i riskanalysen av de incidenter som kan uppstå i dess nätverk och informationssystem bör avse både incidenter som kan ske direkt i dessa, liksom incidenter som kan uppstå utanför leverantörens nätverk och informationssystemen men som kan påverka dem.

Leverantören bör i riskanalysen beakta risker som kan påverka tillgänglighet, riktighet eller konfidentialitet i leverantörens nätverk och informationssystem. Även risker som kan påverka befintliga säkerhetsåtgärder i leverantörens nätverk och informationssystem bör beaktas.

De incidenter som bör ingå i en riskanalys kan exempelvis vara antagonistiska angrepp, tekniska fel, fel orsakade av människan eller naturpåverkan.

Allmänna råd till 3 kap. om informationssäkerhetskrav

1 §

I arbetet med att uppfylla informationssäkerhetskrav bör leverantören ta ställning till vilken typ av övervakning och larmfunktioner som krävs för att åtgärder ska fungera.

Systemloggar bör hanteras med hög säkerhet för att undvika att de riskerar att manipuleras. Loggning bör ske av olika typer av transaktioner, exempelvis av nätverkstrafik mellan segment, nätverkstrafik externt mot internet, förändringar i konfiguration av nätverkets skalskydd eller tilldelning av administratörsrättigheter.

Leverantören bör även införa analysverktyg för att möjliggöra upptäckt av otillåtna aktiviteter, och för att kunna spåra aktiviteter i utredande eller problemlösande syfte. Leverantören bör testa och kalibrera larmfunktioner för att säkerställa att rätt person eller funktion inom organisationen tillhandahålls relevant information.

2 §

Vid kartläggningen och analysen enligt punkt 1 bör leverantören ta ställning till hur kritiskt informationssystemet är för leverantörens tillhandahållande av samhällsviktiga tjänster, liksom hur känslig informationen är som hanteras i informationssystemet.

Leverantören bör hantera hårdvaruinventering enligt punkt 2 genom att upprätta en så kallad ”vitlista” med godkänd hårdvara. Nätverket bör övervakas så att leverantören uppmärksammar om en otillåten enhet kopplas upp mot leverantörens IT eller OT.

Leverantören bör hantera mjukvaruinventering enligt punkt 3 genom att upprätta en så kallad ”vitlista” med godkänd mjukvara. Leverantören bör övervaka sin mjukvara i syfte att möjliggöra upptäckt av en otillåten installering (eller installation) i leverantörens nätverk och informationssystem.

Systemförteckningen kan vara manuellt upprättad eller genererad genom övervakningsapplikationer. Om en övervakningsapplikation används för att identifiera informationssystem och flöden bör applikationen även konfigureras till att larma vid påträffande av nya system och flöden.

3 §

Vid segmentering av nätverk enligt punkt 1, bör leverantören ta ställning till vilken typ av information som finns i segmentet, vilka säkerhetsfunktioner som är införda och om segmentet kommunicerar externt.

För att minimera användande av administrationsrättigheter enligt punkt 2, bör leverantören dels konfigurera sina behörighetsregler så att en administratör bara använder administrativa behörigheter i de fall det är nödvändigt, dels säkerställa att så få personer som möjligt har tillgång till administrativ behörighet.

När leverantören väljer proportionella autentiseringsmetoder enligt punkt 4, bör leverantören ta ställning till

1. vilken behörighetsnivå en användarprofil har,
2. i vilken mån åtkomst sker på distans eller från leverantörens lokaler, samt
3. känsligheten i den information som hanteras via inloggningen.

Leverantören bör använda säkerhetsåtgärder enligt punkt 5, som ger skydd mot skadlig kod i informationssystem inom OT.

Loggning bör ske avseende allt tillträde enligt punkt 6, till den hårdvara och de lokaler vari leverantörens nätverk och informationssystem är beläget.

4 §

Informationssystem bör härdas enligt punkt 1, bland annat genom avstängning av förkonfigurerade tjänster, ändring av lösenord på förinställda användarprofiler och avstängning av schemalagda arbeten.

5 §

Redundans och kontinuitetshantering kan införas på olika tekniska nivåer (t.ex. hårdvara för förvaring, databas, nätverk eller ett helt datacenter), och kan även innebära krav på manuella, analoga arbetssätt.

Allmänna råd till 4 kap. om säkerhetsåtgärder

1 §

För att kunna sänka en risks riskvärde bör åtgärden minska riskens sannolikhet (vara förebyggande) eller minska riskens konsekvens (avse redundans och kontinuitet).

Leverantören bör utvärdera planerade säkerhetsåtgärder för att säkerställa att de inte leder till nya risker i leverantörens nätverk och informationssystem.

2 §

En säkerhetsåtgärd kan påverka en eller flera risker.

4 §

Leverantörens prioritering av säkerhetsåtgärder bör göras utifrån

1. säkerhetsåtgärdens ändamål,
2. det aktuella informationssystemets kritikalitet för tillhandahållande av samhällsviktiga tjänster enligt den analys som ska göras enligt 3 kap. 2 §, punkt 1,
3. informationssystemets tekniska förutsättningar, samt
4. de kostnader och övriga resurser som införandet av säkerhetsåtgärden medför.