SVENSKA KRAFTNÄT

2019/1135

IT-säkerhetskrav för central styrning av FCR

Utgåva: 2.0
Gäller fr.o.m.: 2024-02-20

1 Inledning

Detta regeldokument specificerar de grundläggande informations- och IT-säkerhetskrav som gäller för samtliga underliggande system när leverantör av reserver aktiverar FCR (Frequency Containment Reserve) genom central styrning[1]. Dokumentet avser FCR-produkterna Frekvenshållningsreserv Normaldrift (FCR-N) och Frekvenshållningsreserv Störning (FCR-D).

I alla underliggande system, till exempel resurser i form av teknisk utrustning som ansluts till produktions-, förbruknings- och energilagringsenheter eller grupper för att redovisa driftdata och ta emot styrsignaler, är det väsentligt att säkerställa riktigheten hos den information som utbyts. Förekomster av fel kan annars få betydande påverkan. IT-säkerheten är viktig för att få en robust och förutsägbar FCR-leverans som inte negativt påverkar stabiliteten i kraftsystemet.

Som systemansvarig myndighet har Svenska kraftnät idag inga krav på var komponenter, som krävs för FCR-leveransen, tillverkas. Det är dock viktigt att leverantör av FCR beaktar de krav på säkerhetsskydd som finns i gällande lagstiftning.[2] En leverantör av FCR behöver analysera storleken och funktionen på enheten eller gruppen för att utreda om den skulle kunna påverka Sveriges säkerhet ur säkerhetsskyddslagens perspektiv och, beroende på utkomst i analysen, vidta nödvändiga åtgärder.

Samtliga krav som är beskrivna i detta dokument ska redogöras för i förkvalificeringsansökan i enlighet med den mall Svenska kraftnät tillhandahåller och kompletterande dokument från leverantören.

1.1 Bedömning av IT-säkerheten i leverantörens lösning för central styrning

IT-säkerhetskraven är uppdelade i två delar, en första del där leverantören ska beskriva lösningen i form av exempelvis arkitekturritningar, dataflöden och säkerhetsmekanismer. Den andra delen beskriver de minimikrav lösningen behöver uppfylla. Svenska kraftnät kan inte i förväg formulera specifika, heltäckande krav som gäller alla olika systemlösningar som kan användas av leverantörer av FCR då det är helheten av den totala systemlösningen som är avgörande för nivån av IT-säkerhet. Svenska kraftnät kan därmed behöva ställa ytterligare krav än vad som formulerats i detta dokument beroende på vilken lösning leverantören av reserver använder.

I den granskningsprocess som Svenska kraftnät genomför av aktörens IT-säkerhetslösning granskar Svenska kraftnät i ett första steg att minimikraven

[1] Med central styrning avses en enhet eller grupp som tillhandahåller FCR som styrs genom att frekvensen återkopplas via en central funktion.

[2] Leverantören ska beakta samtliga krav på säkerhetsskydd i lagstiftningen, exempelvis Säkerhetsskyddslagen (2018:585) Säkerhetsskyddsförordningen (2021:955), Polismyndighetens föreskrifter (PMFS 2022:1) men även tillkommande lagstiftning.

uppfylls. Därefter granskar Svenska kraftnät lösningen som helhet utifrån ett angriparperspektiv för att identifiera den svagaste länken. Då identifieras vilken påverkan en specifik angreppsmetodik, en sårbarhet eller frånfall av en enskild komponent kan få på systemlösningens funktion.

För att Svenska kraftnät ska få en komplett bild kan det i samband med granskningen krävas in kompletterande information. Svenska kraftnät gör därefter en sammanvägd bild och godkänner de IT-säkerhetslösningar som finns i leverantörens lösning eller ställer krav på kompletterande åtgärder för att IT-säkerhetslösningarna ska godkännas.

1.2 Leverantörens ansvar

Leverantören av FCR ansvarar ytterst för att informations- och IT-säkerheten hos alla underliggande system håller en miniminivå som överensstämmer med kraven i detta dokument samt vedertagen bransch praxis.

1 Krav: Det skall finnas utpekad ansvarig för IT- och informationssäkerhet. Säkerhetsarbetet ska baseras på att följande är dokumenterat:

   a) Riskanalyser,

   b) Informationssäkerhetspolicy ska finnas,

   c) Leverantören ska presentera hur IT-säkerhetsorganisationen ser ut inom det egna företaget och eventuella dotterbolag samt underleverantörer[3].

   Leverantören ska efter förfrågan från Svenska kraftnät tillgängliggöra dessa dokument för granskning.

2 Krav: Vid förändringar i teknisk infrastruktur och ovan angivna dokument ska Svenska kraftnät meddelas om aktuella förändringar och dess påverkan på IT-säkerheten.

1.3 Systembeskrivning

Information till ansökan:

1 Leverantören ska i ansökan bifoga en arkitekturritning på lämplig nivå över samtliga ingående IT-komponenter i lösningen. Ritningen ska kompletteras med en beskrivande text av ingående komponenter och dataflöden.

2 Ritningen ska minst innehålla information om trafikflöden mellan enskilda komponenter och specifikation av protokoll som används för kommunikation.

3 Information om samtliga ingående hård- och mjukvarukomponenter som har påverkan på förmågan att centralt styra resurser ska specificeras med märke och modell.

[3] Med underleverantörer menas de företag som kan ha en direkt påverkan på förmågan att styra och kontrollera centralt styrda resurser.

4 Information om olika nätverkssegmentering/säkerhetszoner ska vara tydligt markerade.

5 Information om de ingående komponenternas placering ska ingå, exempelvis On-Prem, AWS, Azure eller hos kund.

6 Ansökan ska innehålla en beskrivning av hur åtkomst till olika komponenter/webbsidor sker baserat på olika typer av användare, exempelvis operatörer, kunder och administratörer.

7 Leverantören ska beskriva om det centrala styrsystemet används av flera enheter eller grupper än den aktuella ansökan berör.

8 Leverantören ska göra en risk- och konsekvensbedömning om det centrala IT-systemet går ner eller på annat sätt inte fullgör sin funktion.

9 Leverantören ska i ansökan beskriva om och hur en säkerhetsgranskning (penetrationstest) har genomförts av mjuk och hårdvara i lösningen.

1.4 Redundans

Svenska kraftnät eftersträvar att ha en god tillgänglighet på FCR-resurser för att säkerställa en stabil drift av kraftsystemet. Svenska kraftnät ser därför positivt på system som har en hög redundans. Vid tillhandahållande av centralt styrd FCR är det centrala styrsystemet som hanterar flera anläggningar en känslig komponent för att behålla stabiliteten i leveransen av FCR. Svenska kraftnät har därför valt att kategorisera centralt styrd FCR i två kategorier Kategori A och Kategori B.

Endast en viss del av upphandlad FCR-kapacitet får utgöras av centralt styrd FCR placerad i kategori B. Volymbegränsningen anges på Svenska kraftnäts webbplats[4].

För att placeras i Kategori A skall samtliga krav i detta dokument uppfyllas. Ifall motsägelser förekommer gäller alltid det strängare kravet.

För att placeras i Kategori B skall samtliga krav i detta dokument uppfyllas exklusive punkt 1.4.1. Ifall kraven för Kategori B inte uppfylls tillåts resursen inte att leverera FCR.

1.4.1 Centralt styrt FCR: Kategori A

Krav för att systemet ska hamna i Kategori A

Redundanskrav

1) Samtliga komponenter i servermiljön som har en bäring på förmågan att styra och kontrollera de centralt styrda resurserna ska ha en redundant uppsättning antingen i mjukvaran eller via olika tillgänglighetszoner hos exempelvis en molnleverantör.

    a) Redundansen får inte vara inom samma datacenter eller geografisk plats. Vid eventuellt bortfall av ett datacenter ska flytten av lasten ske utan

[4] Volymbegränsning för centralt styrd FCR placerad i kategori B | Svenska kraftnät (svk.se)

manuella handpåläggningar så snart som möjligt, maximalt inom 5 minuter.

2) Frekvensmätare och hårdvara i lösningen ska ha dubbla anslutningar till nätverket för kommunikation med centrala serverresurser. Det kan lösas via exempelvis olika mobila anslutningar eller kombination mellan fast och mobil anslutning.

    i) Om det inte är tekniskt möjligt att tillhandahålla frekvensmätare med dubbla nätverksanslutningar kan detta krav uppfyllas genom att: Placera minst fem stycken frekvensmätare inom samma elområde på geografiskt åtskilda platser. Där minst tre olika operatörer används för att kommunicera med de fem stycken frekvensmätarna.

    ii) Om det inte är tekniskt möjligt att använda dubbla anslutningar för varje centralt styrd resurs skall minst tre stycken av varandra oberoende operatörer användas för kommunikation med utrustningen. Detta innebär att maximalt 33 % av de centralt styrda resurserna får kommunicera via en enskild operatör.

    iii) Om kommunikationen går via 3G/4G ska en egen APN[5] användas.

3) Frekvensmätaren ska vara redundant i form av minst tre mätare per elområde och ska placeras på tre geografiskt skilda platser.

4) Innan produktionssättning av lösningen ska redundansen praktiskt testas för samtliga ingående komponenter och dokumenteras.

Segmenteringskrav

1) Den centrala mjukvarulösningen som har en bäring på förmågan att styra och kontrollera de centralt styrda resurserna får styra maximalt 70 MW per instans.

2) Den frekvensmätare eller system som mottagare information från en frekvensmätare ska maximalt betjäna 70 MW.

3) Frekvensmätare och övrig infrastruktur ska bara styra system som finns i samma elområde.

4) Samtliga mjukvarukomponenter i servermiljön som har en bäring på förmågan att styra och kontrollera de centralt styrda resurserna ska vara unika uppsättningar per elområde och leverantör av FCR.

Övriga krav på systemlösningen

1. Multifaktorautentisering används för administrativ åtkomst till samtliga mjukvarukomponenter i lösningen, exempelvis administrationsportal för frontend/backend komponenter, servrar och inloggning till molntjänstleverantör.

[5] Genom att använda ett egen APN ges ingen möjlighet till attackyta mot respektive centralt styrt resurs över internet. Detta i kombination med redundans hos flera operatörer ger en god tillgänglighet för samtliga resurser.

2. Vid egen mjukvaruutveckling ska verktygsbaserad sårbarhetsscanning och kodgranskning med tvåhandsfattning[6] användas.
3. Lösningen som helhet ska regelbundet scannas efter sårbarheter och brister. Scanningen ska dokumenteras och allvarliga sårbarheter ska snarast åtgärdas.

1.4.2 Centralt styrt FCR Kategori B

Krav för att systemet ska hamna i Kategori B

1. System som inte uppfyller kraven för kategori A bedöms mot kraven i kategori B.
2. Systemet ska uppfylla samtliga krav som finns i detta dokument utöver de som är specifika för kategori A
3. Frekvensmätare och fysiska anläggningar som styrs ska finnas i samma elområde.
4. Leverantören ska använda minst två stycken frekvensmätare som är placerade på två geografiskt enskilda platser.

1.5 IT-Säkerhetskrav

Nedan områden beskriver de minsta IT-Säkerhetskrav lösningen ska uppfylla.

1.5.1 Mjukvara

1. Leverantören ska ha ett dokumenterat sätt att uppdatera mjukvaran på samtliga ingående komponenter.
2. Åtgärden för att mitigera sårbarheter med CVSS v3 klassning över 8,0 ska göras snarast möjligt.
3. Uppdateringar av programvara ska vara spårbara.

1.5.2 Åtkomstkontroll

1. Leverantören av FCR ska tillse att alla underliggande system skyddas mot obehörig åtkomst genom åtkomstkontroll.
2. Användaråtkomst till systemet ska loggas.
3. Autentiseringen med högt priviligierade kontot ska ske med multifaktorautentisering.
4. Åtkomst till systemets olika delar ska styras utefter arbetsuppgifter.
5. Loggar över användaråtkomst ska sparas på lämplig plats för att möjliggöra analys i ett senare skede.
6. Uppföljning och revidering av höga behörigheter ska ske minst en gång per år.

[6] Med tvåhandsfattning avsesatt koden måste godkännas av utvecklaren och ytterligare en till person med erforderlig kompetens innan den kan checkas in och skjutas ut i den skarpa miljön.

7. Åtkomstkontrollfunktioner skall vara utformade så att autentisering, behörighetsstyrning och spårbarhet säkerställs.
8. Om lösenord måste användas för autentisering i underliggande system ska det ske med unika lösenord.
9. Fabriksinställda användaridentiteter och standardlösenord (s.k. default passwords) ska bytas ut innan underliggande system och resurser tas i drift.
10. Om möjligt ska fjärråtkomst avaktiveras i enheter där behovet inte finns.
11. Lösenordsförteckningar ska skyddas mot obehörig åtkomst.
12. Känsliga delar av systemet bör inte vara åtkomligt för samtliga IP-adresser på internet.

1.5.3 Transportskydd

1. Transportskydd ska tillhandahållas genom kryptografiska funktioner.
2. Kommunikation till och från system som används för central styrning av enhet eller grupp ska loggas och säkerhetsövervakas.
3. Vid användning av TLS skall minst version 1.2 användas och svaga algoritmer och nyckellängder ska avaktiveras.
4. Vid användning av certifikat och SSH nycklar ska det finnas adekvata och dokumenterade säkerhetsåtgärder för att skydda nycklar/certifikat.

1.5.4 Fysiskt och logiskt skydd

1. System för central styrning av enhet eller grupp ska skyddas mot obehörig åtkomst genom fysisk inlåsning.
2. Nätverk ska vara utformat med tillräcklig nivå av segmentering.
3. Leverantören ska beskriva vilka produkter som är tillgängliga utifrån internet

Skadlig kod och intrångsdetektering

1. Leverantören av FCR ska skydda alla underliggande system genom tillfredsställande skydd mot skadlig kod.
2. System för central styrning av enhet eller grupp ska ha någon form av detekteringsfunktion för att upptäcka intrångsförsök och olovliga intrång i systemen.

Incidentrapportering, revision och undantag

Löpande krav: Vid upptäckt av allvarliga IT-säkerhetsbrister eller pågående intrång ska leverantören av FCR skyndsamt meddela Svenska kraftnät om detta.

Exempel på incidenter som ska rapporteras är, påverkan på systemets it-funktionalitet, ransomware attacker, otillbörlig åtkomst till systemet eller läckage av känslig data. Vid betydande säkerhetsbrister ska aktören dessutom se till att

enheten eller gruppen inte tillhandahålls på FCR-marknaden till dess att bristen åtgärdats.

Leverantören av FCR ska tillåta Svenska kraftnät att genomföra säkerhetsrevisioner även efter förkvalificering. Sådan säkerhetsrevision kan genomföras av antingen Svenska kraftnät eller genom en av Svenska kraftnät utsedd tredje part.

Undantag från ovanstående krav kräver i varje enskilt fall godkännande från Svenska kraftnät och ansökan ska föregås av en egen analys kring vilka risker som kvarstår.