Nätkoder för cybersäkerhet på gång – förslag från ACER

Under de senaste åren har många nya bestämmelser, som NIS-direktivet och striktare nationell säkerhetslagstiftning, implementerats. År 2022 väntas de nya obligatoriska EU-riktlinjerna om nätkoder för cybersäkerhet träda i kraft. Här följer ACER:s förslag i sammandrag.

ACER har tagit fram ett förslag på ramriktlinje för cybersäkerhet; ”Riktlinje för sektorsspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden”. Förslaget innehåller principer för EU-gemensamma regler bland annat om gränsöverskridande riskhantering, cybersäkerhet, informationsutbyte, incidenthantering och krishantering.

Betydelsen av cybersäkerhet ökar med den tekniska utvecklingen inom IoT och AI, och ett mer digitalt och sammankopplat energisystem. Det moderna energisystemet är inte begränsat av nationella gränser. Fler och fler system kopplas ihop när samhället elektrifieras. Som ett resultat kan cyberangrepp få gränsöverskridande kaskadeffekter på hela samhället.

Digitaliseringen i verksamheterna betyder att vi blir mer sårbara och måste sätta oss in i hur vi använder tekniken både smart och säkert. Olika enheter och deras underliggande system, som ofta blandar gammal och nyare teknik, har sårbarheter. När de utnyttjas felaktigt eller av obehöriga, kan de underminera verksamheters leverans- och distributionsförmåga och användas för cyberangrepp.

Vem berörs av det nya lagförslaget?

Alla som producerar och distribuerar el och har känslig information som är sårbar för cyberangrepp berörs. Cybersäkerhet är direkt avgörande för nationens – och världens – trygghet och säkerhet. Cyberangrepp mot kritisk infrastruktur kan vara katastrofala och orsaka fysisk skada eller allvarliga störningar. Alla som bedriver en kritisk verksamhet måste vidta åtgärder för att förbättra sin cybersäkerhet och minska risken att drabbas av cyberangrepp med bibehållen leveranssäkerhet.

ACER:s utkast bygger på NIS-2 direktivets förslag på definitioner av kritiska entiteter. Men här finns möjlighet att tycka till och påverka omfattningen. Det är även av vikt att beakta underleverantörer och små organisationer som kan fungera som kanaler för angripare på större verksamheter.

Hur ska elflödet skyddas?

Fokus i utkastet är att använda riskanalys och en helhetssyn, samt anpassa systemet till de unika förhållandena inom energisektorn med branschspecifika lagkrav, men också extern övervakning i EU. Det finns flera viktiga åtgärder att följa för att minska riskerna och hålla företagets data säkra. I utkastet föreslår ACER tre steg:

1. Undersök och avgör var säkerhetsrisker ligger i din organisation genom Electricity Cybersecurity Risk Index (ECRI).

3. Implementera rätt verktyg som kontinuerligt övervakar och identifierar sårbarheter samt varnar anställda så att din organisation kan agera snabbt för att minska riskerna.

4. Implementera grundläggande kontroller och grundläggande säkerhetshygien. Uppfyllandet av fler säkerhetskrav ökar i korrelation med storleken på verksamheten.

Tre viktiga förslag som påverkar verksamheten

1) En SOC-tjänst (Security Operation Center) hjälper att få kontroll, överblick och upptäcka säkerhetsincidenter som påverkar elflödena. Det ger också stöd att prioritera incidenter, tolka rapporter och fatta rätt beslut om åtgärder. I förslaget ställs krav på kontinuerlig bevakning och analys av dataflöden. Nackdelen med förslaget är att flertalet aktörer i branschen idag saknar en SOC-organisation. Här finns incitament för att bygga upp en säkerhetsorganisation och/eller köpa in tjänsten av en underleverantör. Fördelar med att använda en SOC-tjänst:

    - Skyddande av nätverk och data från obehörig åtkomst
    - Förbättrad kontinuitetshantering och leveransförmåga
    - Snabbare återhämtning i händelse av intrång
    - Förbättrad tillit och förtroende från samhällsintressenter

2) Certifieringskrav på produkter. Kritiska enheter inom energisektorn som använder digitala tjänster ska uppfylla minimistandarderna inom nätverkssäkerhet och dataskydd för produkter. I förslaget finns krav på certifiering. Frågan är om dessa krav uppfylls genom att göra en ”Cyber Essentials för dataskydd” eller om det är nödvändigt med krav på standardcertifieringar? Certifieringar i sig kanske inte är en garanti för högre säkerhetsnivå i sektorn, och innebär kostnadsökningar för företag.

3) Incidentrapportering, för att göra framsteg och ge ”en morot” krävs en tydlig definition när rapportering ska ske och feedback från CSIRT (motsvarande CERT i Sverige). Syftet bör vara att lära av incidenter och ge feedback om säkerhetsåtgärder, incidentprocesser, kompetensutvecklingsåtgärder för personal och uppdatering av rutiner. Annars försvinner mycket av kunskapen och erfarenheten från incidenter och misstagen lär göras om. Nya sårbarheter kan också upptäckas, eller behovet av nya eller förbättrade säkerhetsåtgärder under hanteringen av en incident.

Lämna synpunkter senast 18 juni

Läs medlemsnyhet från Energiföretagen Sverige från den 25 maj 2021 om hur ni kan lämna svar på ACER:s utkast och bidra till branschens gemensamma syn här.