NC-SPECTRUM

Kraftberedskapsforskriften kapittel 6 og 7, IT-sikkerhet og nettverk

Gjeldende forskrift

Den gjeldende forskriften ble endret med effekt fra 01.01.2019. Det vil si at endringer som ble annonsert i november 2018, ble satt i effekt under to måneder senere. Her fokuserer vi på de punktene som særlig berører IT-sikkerhet, et tema som har fått betydelig økt fokus i forskriften, og som vil ha et mye større fokus i fremtidige tilsyn og revisjoner.

Det er innført noen systemmessige endringer som grunnlag for hvordan man skal forholde seg til beredskap. Et eksempel er kravet til å etablere systemer og rutiner i tråd med NSM sine grunnprinsipper for IKT-sikkerhet. I tillegg kommer endringer i den enkelte paragraf og bokstav. På siste side finner du hele *§ 6-9. Digitale informasjonssystemer*.

Anbefalte løsninger fra NC-Spectrum AS

Det kan være vanskelig å få oversikt over hva de nye kravene egentlig innebærer av endringer, og hva som kan gjøres for å møte dem på en god måte.

NC-Spectrum kan hjelpe KBO-enheten til å tolke de ulike punktene, og komme med forslag til gode og effektive løsninger. På de neste sidene ser du en oversikt over den enkelte bokstav i § 6-9, og hva NC-Spectrum kan bidra med på det enkelte punkt. Det er likevel viktig å understreke at man bør gjennomføre en kontroll av dagens situasjon i selskapet før man går løs på disse oppgavene; kanskje er mange av dem dekket allerede. Vi kan, sammen med kunden, utarbeide en tilstandsrapport i forhold til oppfyllelse av kravene i kraftberedskapsforskriften.

Paragraf	**Tekst**	
§ 6-9 a)	*Identifisere og dokumentere* *Virksomheter skal identifisere og dokumentere verdier, leveranser, tjenester, systemer og brukere i sine digitale informasjonssystemer. Dokumentasjonen skal holdes oppdatert.*	
Produkt	**Innhold**	**Pris**
Nettverks-overvåking	For å holde oversikt over nettverket bør man ha et verktøy for nettverksovervåking. NC-Spectrum anbefaler SolarWinds som overvåkingsverktøy. Vi er norsk reseller av SolarWinds og hjelper til å finne den løsningen som passer best for kundens behov. Vi har sertifiserte teknikere som kan bistå med opplæring, konfigurasjon og eventuelt drift av løsningen.	SolarWinds: Avhengig av antall og størrelse på moduler

Paragraf	**Tekst**	
§ 6-9 b)	*Risikovurdering* *Virksomheter skal gjennomføre risikovurdering ved systemendringer. Risikovurderingen skal holdes oppdatert.*	
Produkt	**Innhold**	**Pris**
Risikovurdering	NC-Spectrum kan gjennomføre risikovurderinger for å kartlegge trusler og potensielle konsekvenser av uønskede hendelser. I risikovurderingen beskriver vi også viktige forebyggende tiltak.	Faktureres pr medgått time

Paragraf	Tekst	
§ 6-9 c)	*Sikre og oppdage* *Virksomheter skal sikre sine digitale informasjonssystemer for å motstå eller begrense skade fra uønskede hendelser. Virksomheter skal overvåke sine digitale informasjonssystemer slik at uønskede hendelser oppdages og registreres. Virksomheten skal varsle uønskede hendelser i sine digitale informasjonssystemer til den beredskapsmyndigheten bestemmer.*	
Produkt	**Innhold**	**Pris**
Nettverks-overvåking IDS Penetrasjons-testing	«Å sikre» handler blant annet om å ivareta sikkert design av IKT-miljø, kontrollere dataflyt, og etablere hensiktsmessig logging. Her er det, som i bokstav a), hensiktsmessig å benytte seg av et nettverksovervåkingsverktøy som SolarWinds. I «å oppdage» er det nødvendig å ha en aktiv IDS (intrusion detection system) ute i nettverket. NC-Spectrum leverer IDS som overvåker nettverk og varsler ved potensiell ondsinnet trafikk eller brudd på policy-regler. Vi kan bistå med installasjon, tilpasning og drift av IDS til en svært konkurransedyktig pris Penetrasjonstesting (også kalt *inntrengningstest* eller *pentest*) omtales i veileder til forskriften som en del av grunnprinsippet i kravet til å «oppdage», og skal gjennomføres i alle KBO'er. NC-Spectrum har spesialister som årlig gjennomfører mange pentester, og kan tilby dette med høy kvalitet til en god pris. Nivået i testen avtales mellom kunde og konsulent.	SolarWinds: Avhengig av antall og størrelse på moduler IDS: 12.000,- pr måned Pentest: faktureres pr medgått time

Paragraf	Tekst	
§ 6-9 d)	*Håndtere og gjenopprette* *Virksomheter skal håndtere uønskede hendelser i sine digitale informasjonssystemer og gjenopprette normaltilstand uten ugrunnet opphold.*	
Produkt	**Innhold**	**Pris**
IKT-sikkerhetsøvelse Hendelse-håndtering	Bokstav d) viser til at virksomheten må ha en plan for gjenoppretting til normaltilstand dersom det forekommer en uønsket hendelse. NC-Spectrum tilbyr IKT-sikkerhetsøvelser der det gjennomgås ulike scenarioer av ekstraordinære situasjoner. Deltakerne på øvelsen lærer hvordan man best mulig kan håndtere ulike situasjoner. For virksomheter som har NOC/SOC-avtale med NC-Spectrum, har vi et eget team som kan bistå med håndtering av hendelser og gjenoppretting til normaltilstand.	Faktureres pr medgått time

Paragraf	Tekst	
§ 6-9 e)	*Tjenesteutsetting* *Virksomheter skal sørge for at sikkerhetsnivået opprettholdes eller forbedres ved utsetting av tjenester.*	
Produkt	**Innhold**	**Pris**

Rådgivning og dokumentasjon	Ved tjenesteutsetting er det nødvendig med kompetanse på anskaffelse og IKT-sikkerhet. NC-Spectrum bistår gjerne med rådgivning knyttet til tjenesteutsetting. Vi bistår også med dokumentasjon av eksisterende system, hvilket det er viktig å ha på plass før man benytter seg av tjenesteutsetting.	Faktureres pr medgått time

Paragraf	**Tekst**	
§ 6-9 f)	*Sikkerhetsrevisjon* *Virksomheter skal jevnlig gjennomføre revisjoner av iverksatte sikringstiltak for digitale informasjonssystemer. Revisjoner skal påse at tiltakene faktisk er etablert og fungerer etter sin hensikt. Hver revisjon kan ta for seg deler av sikringstiltakene.*	
Produkt	**Innhold**	**Pris**
Sikkerhets-revisjon	NC-Spectrum tilbyr sikkerhetsrevisjoner for e-verk. Revisjonen gir en oversikt over dagens situasjon for virksomhetens sikkerhetsnivå. Den beskriver også ulike tiltak som kan gjennomføres for å øke sikkerhetsnivået. Alle resultatene fra revisjonen dokumenteres.	Faktureres pr medgått time

NC-SPECTRUM

§ 6-9. Digitale informasjonssystemer

§ 6-9. Digitale informasjonssystemer

Virksomheter skal sikre digitale informasjonssystemer slik at konfidensialitet, integritet og tilgjengelighet ivaretas.

Det er den enkelte virksomhets ansvar å planlegge, gjennomføre og vedlikeholde sikringstiltak etter det digitale informasjonssystemets type, oppbygging og funksjon.

Virksomheter skal ha en grunnsikring for digitale informasjonssystemer i henhold til anerkjente standarder og normer, herunder:

a. *Identifisere og dokumentere*
   Virksomheter skal identifisere og dokumentere verdier, leveranser, tjenester, systemer og brukere i sine digitale informasjonssystemer. Dokumentasjonen skal holdes oppdatert.

b. *Risikovurdering*
   Virksomheter skal gjennomføre risikovurdering ved systemendringer. Risikovurderingen skal holdes oppdatert.

c. *Sikre og oppdage*
   Virksomheter skal sikre sine digitale informasjonssystemer for å motstå eller begrense skade fra uønskede hendelser. Virksomheter skal overvåke sine digitale informasjonssystemer slik at uønskede hendelser oppdages og registreres. Virksomheten skal varsle uønskede hendelser i sine digitale informasjonssystemer til den beredskapsmyndigheten bestemmer.

d. *Håndtere og gjenopprette*
   Virksomheter skal håndtere uønskede hendelser i sine digitale informasjonssystemer og gjenopprette normaltilstand uten ugrunnet opphold.

e. *Tjenesteutsetting*
   Virksomheter skal sørge for at sikkerhetsnivået opprettholdes eller forbedres ved utsetting av tjenester.

f. *Sikkerhetsrevisjon*
   Virksomheter skal jevnlig gjennomføre revisjoner av iverksatte sikringstiltak for digitale informasjonssystemer. Revisjoner skal påse at tiltakene faktisk er etablert og fungerer etter sin hensikt. Hver revisjon kan ta for seg deler av sikringstiltakene.