JULI 2024

Skärpta krav på *cybersäkerhet*

VINGE

Mot bakgrund av det allvarliga säkerhetspolitiska läget och den snabbt ökande digitaliseringen införs nu EU-direktiv som ställer ökade krav på informations- och cybersäkerhet. De nya reglerna föreslås införas i Sverige genom en ny lag – Cybersäkerhetslagen. Lagen innebär skärpta krav och allvarliga ekonomiska konsekvenser om man bryter mot bestämmelserna.

Bakgrund

NIS-direktiven syftar till att uppnå en hög gemensam cybersäkerhetsnivå i hela unionen. Det första direktivet antogs 2016. Säkerhetsläget har sedan dess förvärrats och EU har identifierat att hotbilden mot informations- och nätverkssystem har ökat. EU har därför antagit ett nytt direktiv, NIS2-direktivet, som innehåller skärpta krav på cybersäkerhet. Direktivet börjar tillämpas den 18 oktober 2024 och ska nu införas i svensk lag.

Förslag till ny lag om cybersäkerhet

Tidigare i vår var utredningen kring vilka anpassningar som behöver göras i svensk rätt med anledning av direktivet klar. Utredningen (SOU 2024:18) föreslår att det ska införas en ny lag om cybersäkerhet (”**Cybersäkerhetslagen**”). Den nya lagen föreslås träda i kraft 1 januari 2025 (utan någon övergångsperiod).

Kommer ert bolag omfattas av de nya bestämmelserna?

Cybersäkerhetslagen föreslås gälla både för offentliga och privata aktörer (kallas verksamhetsutövare i lagen), inom en rad sektorer. Bestämmelserna i Cybersäkerhetslagen kommer att gälla ert bolag om följande förutsättningar är uppfyllda:

1. **bolaget bedriver, helt eller delvis, verksamhet inom en av de listade sektorerna**: Cybersäkerhetslagen gäller för aktörer som bedriver verksamhet inom någon av de 18 sektorer som pekas ut av NIS2 och Cybersäkerhetslagen,
2. **etablering i Sverige**: som huvudregel gäller lagen för verksamheter som är etablerade i Sverige, och
3. **bolaget uppfyller kraven för ”medelstort företag”**: små bolag kommer som huvudregel inte att beröras, mer om det nedan.

Sektorer som omfattas

Cybersäkerhetslagen föreslås omfatta 18 olika sektorer. Bedömningen om ett bolag anses verksam inom de relevanta sektorerna är ibland svår. Kraven kommer att gälla för hela verksamheten och innebär alltså om någon del av företagets verksamhet bedrivs inom en av de utpekade sektorerna så ”smittas” hela bolaget, d.v.s. hela bolagets verksamhet kommer då att omfattas av reglerna.

De sektorer som kommer att omfattas är:

Energi

Inkluderar bland annat bolag som säljer el till kund (både slutkund och återförsäljare), laddningsoperatörer, operatörer av fjärrvärme och fjärrkyla och aktörer aktiva inom produktion, leverans etc. inom gas och vätgas.

Transporter

Inkluderar bland annat flygbolag, flygplatser, aktörer inom järnvägstransport inklusive tjänsteleverantörer, operatörer av intelligenta transportsystem och sjöfartsföretag inom persontrafik och godstrafik.

Bankverksamhet

Kreditinstitut, dvs företag vars verksamhet består i att från allmänheten ta emot insättningar eller andra återbetalbara medel och att bevilja krediter för egen räkning.

Finansmarknadsinfrastruktur

Börser och handelsplattformar.

Hälso- och sjukvård

Inkluderar bland annat sjukhus och kliniker, bolag som utvecklar eller tillverkar läkemedel eller medicintekniska produkter som Socialstyrelsen listat som kritiska vid hot mot folkhälsan.

Dricksvatten

Inkluderar verksamheter som hanterar dricksvattenledningar och nät, men också företag som distribuerar flaskvatten till användare eller livsmedelsföretag.

Avloppsvatten

Företag som hanterar avloppsvatten, hushållsspillvatten eller industrispillvatten.

Digital infrastruktur

Inkluderar bland annat leverantörer av molntjänster, datacentraltjänster och nätverk, samt tillhandahållare av betrodda tjänster, allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster.

Verksamhetsutövare som erbjuder allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster behöver **inte** vara etablerade i Sverige för att omfattas av lagen utan det är tillräckligt att verksamhetsutövaren erbjuder tjänster i Sverige.

Förvaltning av IKT-tjänster

Verksamhet som erbjuder tjänster som rör installation, förvaltning, drift eller underhåll av produkter, nät, infrastruktur, system etc. inom information och kommunikationsteknik (mellan företag).

Offentlig förvaltning

Offentliga verksamhetsutövare såsom statliga myndigheter, med vissa undantag, regioner och kommuner.

Rymden

Operatörer av markbaserad infrastruktur som stöder tillhandahållandet av rymdbaserade tjänster såsom satellitkommunikation, positionerings- och tidstjänster.

Post- och budtjänster
Tillhandahållare av tjänster som är en del av post- och budleveranskedjan, såsom insamling, sortering, transport och överlämnande av postförsändelser.

Avfallshantering
Företag vars huvudsakliga näringsverksamhet är avfallshantering.

Tillverkning, produktion och distribution av kemikalier
Företag som tillverkar, producerar eller distribuerar vissa kemikaliska ämnen, blandningar eller varor, enligt REACH-förordningen.

Produktion, bearbetning och distribution av livsmedel
Livsmedelsföretag som bedriver grossisthandel och industriell produktion och bearbetning.

Tillverkning av vissa produkter
Inkluderar tillverkare av en bred grupp av produkter, exempelvis medicinska produkter, datorer, elektronikvaror, optik, elmotorer, generatorer, motorgeneratorer, hushållsapparater, släpfordon och påhängsvagnar.

Digitala leverantörer
Inkluderar leverantörer av marknadsplatser online där konsumenter kan ingå köpavtal med andra konsumenter eller med näringsidkare, sökmotorer och sociala media.

Forskning
Organisationer som riktar in större delen av sin verksamhet på forskning i syfte att utnyttja sina resultat i kommersiella syften.

Omfattas offentliga aktörer?

Ja, *offentlig förvaltning* är en av de sektorer som omfattas av förslaget till Cybersäkerhetslagen. Det medför att i princip alla myndigheter, såväl kommuner, regioner som statliga myndigheter omfattas. Förslaget innehåller dock några undantag så som exempelvis regeringen, domstolar, Riksbanken och region- och kommunfullmäktige.

Storlekskravet

För enskilda verksamhetsutövare gäller som huvudregel ett storlekskrav med innebörd att verksamheten, för att omfattas av lagen, måste:

1. sysselsätta minst 50 personer; *eller*
2. ha en årsomsättning som överstiger 10 miljoner euro.

Det betyder att små företag som utgångspunkt inte kommer att beröras. För att avgöra om ett företag omfattas av Cybersäkerhetslagen behöver man alltså göra en storleksbedömning.

Storleken mäts genom antalet anställda och omsättning/balansomslutning.

Tänk på att det är hela koncernens omsättning som räknas in!
Även omsättningen för partnerföretag ska läggas till. Partnerföretag är bolag som verksamhetsutövaren har en kapital- eller röstandel på minst 25 procent.

Innebörden av detta blir att även företag som inte når upp till storlekskravet som egen juridisk person kan göra det på grund av sambandet med exempelvis ett moderbolag.

Vissa särskilt utpekade enskilda verksamhetsutövare omfattas dock oavsett storlek. Myndigheten för samhällsskydd och beredskap (MSB) kommer också att ha möjlighet att peka ut vissa särskilt kritiska mindre verksamheter. Enskilda verksamhetsutövare som enbart

bedriver säkerhetskänslig verksamhet, brottsbekämpning eller erbjuder tjänster till myndigheter som gör det, är undantagna.

Cybersäkerhetslagen föreslås innehålla ett antal undantag till storlekskravet som gör att även mindre aktörer kan omfattas i vissa fall. Exempelvis gäller det om aktören är av särskild betydelse på regional eller nationell nivå, om en störning avseende den tjänst som aktören tillhandahåller kan få påverkan på människors liv och hälsa, eller om aktören tillhandahåller allmänna elektroniska kommunikationsnät eller är en tillhandahållare av betrodda tjänster (exempel på betrodda tjänster är elektronisk legitimation eller certifikat för autentisering av webbplatser).

Även för myndigheter föreslås att storlekskravet inte ska gälla, utan de omfattas i princip alltid av de nya reglerna. Kommuner föreslås dock endast omfattas om de uppfyller storlekskravet.

Verksamheter som inte omfattas – indirekt påverkan?

Även för bolag som inte omfattas av Cybersäkerhetslagen kan lagen få en indirekt effekt. Det hänger samman med att de verksamhetsutövare som omfattas av lagen har en skyldighet att vidta riskhanteringsåtgärder i förhållande till sina leverantörer. För leverantörer till bolag eller myndigheter som omfattas kommer alltså lagen att indirekt få effekt.

Frågan är hur många led i leveranskedjan som avses. Utredningens bedömning är att de verksamhetsutövare som omfattas endast behöver vidta riskhanteringsåtgärder i förhållande till dess direkta leverantörer eller tjänsteleverantörer, d.v.s. endast ett led i leveranskedjan.

De viktigaste bestämmelserna i Cybersäkerhetslagen

Anmälningsskyldighet

En verksamhetsutövare som omfattas av lagen ska anmäla sig till sin tillsynsmyndighet och lämna uppgifter om bland annat identitet, kontaktuppgift och verksamhet. Vilken tillsynsmyndighet som anmälan ska ske till varierar utifrån vilken sektor som är aktuell. De sektorer som redan omfattas av den befintliga lagstiftningen kommer enligt förslaget ha samma tillsynsmyndigheter som tidigare samtidigt som ytterligare tillsynsmyndigheter tillkommer. Indirekt innebär anmälningskravet att alla organisationer behöver göra en bedömning om man omfattas av Cybersäkerhetslagen eller inte.

Skyldighet att vidta riskhanteringsåtgärder

Den mest centrala delen av lagförslaget är att det innehåller krav på att verksamhetsutövare ska vidta riskhanteringsåtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Åtgärderna ska utgå från en riskanalys, vara proportionella och löpande utvärderas. Åtgärderna ska omfatta följande områden:

1. incidenthantering,
2. kontinuitetshantering,
3. säkerhet i leveranskedjan,
4. säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem inklusive hantering av sårbarheter och sårbarhetsinformation,
5. strategier och förfaranden för användning av kryptografi och kryptering,
6. personalsäkerhet,
7. strategier för åtkomstkontroll och tillgångsförvaltning,
8. säkrade lösningar för kommunikation, och
9. lösningar för autentisering.

Innebörden av informationssäkerhetsarbete är att skydda uppgifter som lagras, behandlas, hämtas eller överförs. De ska skyddas utifrån aspekterna tillgänglighet, autenticitet, riktighet och konfidentialitet. Det betyder att allt arbete som syftar till att säkerställa systemen, tjänsterna och informationen som lagras, behandlas eller överförs genom dem omfattas. Även fysisk hantering av sådant som kan påverka systemen påverkas alltså, så som exempelvis tillträde till lokalerna.

Skyldighet att rapportera incidenter

Utredningen föreslår en skyldighet att rapportera ”betydande incidenter” till MSB. Detta innebär att verksamhetsutövaren ska lämna en varning om incidenten till MSB inom 24 timmar efter det att verksamhetsutövaren fått kännedom om incidenten. Vidare ska en incidentanmälan göras inom 72 timmar och en slutrapport ska upprättas inom en månad.

Utredningen föreslår följande definitioner av ”betydande incident”:

1. En incident som orsakat eller kan orsaka allvarlig driftstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren, eller,
2. En incident som har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada.

Ledningens ansvar

Förslaget pekar tydligt ut att verksamhetsutövarens ledningsorgan är ansvarigt för att godkänna och övervaka genomförandet av riskhanteringsåtgärderna. Med ledningsorgan avses för aktiebolag styrelsen, vd och vice vd.

Innebörden av ansvaret för ledningsorganen är att det ska vara möjligt att vidta åtgärder eller rikta sanktioner mot denna personkrets. Exempelvis innebär förslaget att det ska vara möjligt att meddela förbud för denna personkrets att utöva en ledningsfunktion om lagen inte följs.

Vidare ställs krav att ledningen ska genomgå utbildning i riskhanteringsåtgärder medan anställda ska erbjudas liknande utbildning.

Sanktioner

Tillsynsmyndigheterna får besluta om sanktionsavgifter vid överträdelser av Cybersäkerhetslagen. Enligt utredningens förslag ska sanktionsavgifter höjas jämfört med nuvarande lagstiftning. Den maximala avgiften blir det högsta av:

1. **2 procent** av verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. **tio miljoner euro**.

För myndigheter föreslås den maximala sanktionsavgiften bli tio miljoner kronor.

Tillsynsmyndigheterna ska också kunna förelägga en verksamhetsutövare att vidta rättelse, att offentliggöra information om överträdelser av lagens bestämmelser och att informera personer och bolag som kan påverkas av ett betydande cyberhot. Tillsynsmyndigheterna föreslås också under vissa omständigheter få genomföra säkerhetsrevision och säkerhetsskanning hos de verksamhetsutövare som omfattas av lagen.

Hur kan verksamheter förbereda sig redan nu?

- Analysera om er verksamhet eller någon av era kunder kan förväntas omfattas av bestämmelserna.
- Identifiera relevant tillsynsmyndighet och bevaka nyheter angående förfaranden för anmälningsskyldigheten.

- Ta fram en tydlig ansvarsstruktur för bevakning och efterlevnad av de nya lagkraven. Kom ihåg ledningsansvaret!
- Inventera befintliga rutiner för incidenthantering och incidentrapportering för att identifiera om de behöver uppdateras utifrån de nya kraven. Om bolaget inte har sådana rutiner behöver det tas fram.
- Inventera säkerhet i leveranskedjan – avtal kan behöva omförhandlas för att ställa krav på leverantörers cybersäkerhet.

Vad händer härnäst?

Under hösten förväntas utredningen komma med slutbetänkande angående cybersäkerhet, och därefter kommer regeringen lägga fram en proposition kring Cybersäkerhetslagen. I övrigt förväntas förtydligande förordningar och föreskrifter relaterat till implementeringen av NIS2-direktivet och Cybersäkerhetslagen.

Vinge bevakar kontinuerligt utvecklingen så kontakta oss gärna om du vill veta mer.

Kontakt

Sofie Nordgren
Delägare, Advokat
sofie.nordgren@vinge.se

Lisa Bourghardt
Counsel, Advokat
lisa.bourghardt@vinge.se

Henrik Borna
Delägare, Advokat
henrik.borna@vinge.se