2027

SOFF

Rapport

Hur NIS2 och CER påverkar försvars- och säkerhetsföretag i Sverige

Säkerhets- och försvarsföretagen
(SOFF)

Inledning

I en tid då digitalisering och teknologisk utveckling fortskrider i snabb takt blir cybersäkerhet allt viktigare, särskilt för företag inom försvars- och säkerhetssektorn. Dessa företag hanterar vanligen känslig information och kritisk infrastruktur som utgör attraktiva mål för cyberangrepp. Utöver cyberhot möter företag också andra ökande hot, såsom andra former av hybridhot, antagonistiska hot och naturkatastrofer.

Europeiska unionen (EU) har mot denna bakgrund infört en rad lagstiftningsåtgärder, där NIS2 (Network and Information Security 2 Directive) och CER (Critical Entities Resilience Directive) utgör två centrala komponenter för att förbättra resiliensen, cybersäkerheten och svarskapaciteten i händelse av cyberincidenter mot företag och andra hot eller incidenter mot kritisk verksamhet. Syftet med direktiven är att uppnå en hög gemensam cybersäkerhetsnivå respektive säkerställa motståndskraften av samhällsviktig verksamhet. I denna sammanfattning diskuteras hur de två direktiven påverkar svenska företag inom försvars- och säkerhetssektorn och hur företagen kan förbereda sig för att efterleva de nya kraven.

Bakgrund

NIS2-direktivet

NIS2-direktivet antogs officiellt av EU den 27 december 2022 och ska ersätta det första NIS-direktivet. Syftet med NIS2 är att uppnå en hög gemensam cybersäkerhetsnivå i EU, bland annat genom att ställa högre krav på riskhanteringsåtgärder och incidentrapportering för fler sektorer och organisationer. Direktivet träder i kraft den 18 oktober 2024.

En av de mest påtagliga förändringarna i NIS2 – jämfört med det ursprungliga NIS-direktivet – är den utökade omfattningen. Betydligt fler aktörer omfattas av NIS2 då antalet sektorer ökar från sju till arton, vilket innebär att fler företag måste anpassa sina åtgärder för att uppfylla de nya kraven. NIS2 innebär också att hela verksamheten kommer att omfattas av lagstiftningen och att högre krav ställs på tillsynsåtgärder, rapportering av cybersäkerhetsincidenter och riskhantering.

CER-direktivet

CER-direktivet antogs av EU i december 2022 och är en central del av EU:s strategi för att stärka resiliensen hos samhällsviktiga verksamheter. Syftet är att kritiska entiteter ska kunna motstå hot och angrepp samt snabbt återhämta sig från störningar såsom naturkatastrofer, hybridhot och antagonistiska hot. Direktivet ersätter det tidigare ECI-direktivet (European Critical Infrastructures) och träder i kraft den 18 oktober 2024.

CER-direktivet inkluderar ett bredare spektrum av kritiska sektorer än ECI-direktivet och omfattar sektorer såsom energi, digital infrastruktur, transport och rymd. Medlemsstaterna ska enligt direktivet vidta åtgärder för att säkerställa obehindrad tillgång till vissa samhällsviktiga tjänster och identifiera samt skydda kritiska enheter genom att bland annat säkerställa genomförande av robusta riskbedömningar och motståndskraftiga åtgärder.

Implementering av direktiven i svensk rätt

Direktiv, som NIS2 och CER-direktiven, binder medlemsstaterna och måste införlivas i nationell rätt. I mars 2024 överlämnade därför Utredningen om genomförande av NIS2- och CER-direktiven bland annat ett förslag till en ny cybersäkerhetslag (se SOU 2024:18).

I september redovisade utredningen sitt slutbetänkande avseende motståndskraft i samhällsviktiga tjänster (se SOU 2024:64). I slutbetänkandet föreslås en ny lag och förordning om motståndskraft hos kritiska verksamhetsutövare.

Lagändringarna föreslås träda i kraft i januari respektive augusti 2025. Svensk lagstiftare måste säkerställa att nationell reglering ställer åtminstone samma krav som direktiven gör. Därtill kan lagstiftaren välja att reglera om ytterligare skyldigheter.

I utredningen anges att den svenska lagstiftningen, med något enstaka undantag, inte föreslår några skyldigheter utöver vad som följer av direktiven. Samtidigt kan det noteras att regeringen har en hög ambition för cybersäkerhetsområdet och att flera remissinstanser kritiserar olika former av så kallade överimplementeringar (dvs. när lagstiftaren föreslår mer långtgående krav än vad direktiven kräver).

Påverkan på svenska företag inom försvar och säkerhet

Högre krav på riskanalys och riskhantering till följd av NIS2

Till följd av NIS2-direktivet kommer det att ställas höga krav på försvars- och säkerhetsföretagattutifrånett allriskperspektiv vidta åtgärder för att skydda nätverks- och informationssystem samt dess fysiska miljöer mot incidenter. En uppräkning av minimikraven på vilka åtgärder som ska vidtas finns i artikel 21(2) i NIS2-direktivet.

Bland annat ska företagen ha strategier för riskanalys och informationssystemens säkerhet samt strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärderna.

Andra åtgärder som kravställs inbegriper incidenthantering, driftskontinuitet samt strategier och förfaranden för användning av kryptografi och, när så är lämpligt, kryptering. För att stärka säkerheten måste företag även säkerställa sina leveranskedjor till sina direkta leverantörer. Det finns också krav på åtgärder för personalsäkerhet.

Utökade rapporteringsskyldigheter till följd av NIS2

En viktig aspekt i NIS2 är kraven på rapportering som regleras i artikel 23.

Företag måste inrätta effektiva rapporteringssystem för att snabbt kunna anmäla cybersäkerhetsincidenter till relevanta myndigheter – en varning ska lämnas inom 24 timmar från att verksamhetsutövaren fått kännedom om den betydande incidenten, en incidentanmälan ska göras inom 72 timmar och en slutrapport inom en månad.

Strängare tillsyn till följd av NIS2

Med de nya reglerna tillkommer strängare tillsyns- och efterlevnadskontrollåtgärder. Företag som faller inom kategorin ’väsentliga entiteter’ kan bli föremål för regelbundna inspektioner och revisioner för att säkerställa att de kommande nationella regleringarna inom området efterlevs. Förfarandet för tillsyn kommer att regleras närmre i nationell lagstiftning.

I förslaget till ny cybersäkerhetslag föreskrivs grundläggande regler för tillsyn vilka utvecklas närmre i förslag till förordning om cybersäkerhet. Bolag som omfattas av flera sektorer kan så som förslaget lyder bli föremål för tillsyn av flera olika myndigheter. Tillsynen kommer att innebära en ökad administrativ börda, då företag bland annat måste dokumentera och på begäran kunna tillhandahålla information som tillsynsmyndigheten efterfrågar. Samtidigt kan tillsynen utgöra stöd för leverantörer i deras eget säkerhetsarbete.

Kostnader för den som inte efterlever kraven i NIS2

Kostnaderna för företag som inte uppfyller de krav som ställs på dem riskerar att bli höga. För överträdelser av NIS2 kan sanktionsavgifter för väsentliga entiteter uppgå till högst 10 miljoner euro eller 2 procent av organisationens totala globala omsättning och för viktiga entiteter högst 7 miljoner euro eller högst 1,4 procent av organisationens totala globala omsättning (den största gäller i respektive fall).

Utökat ansvar för styrelsen och VD:n enligt NIS2

En signifikant ändring till följd av NIS2 är att ledningen (styrelsen och VD:n) får ett personligt ansvar för överträdelser av kraven på riskhanteringsåtgärder som ställs på enskilda verksamheter. Ledningen ska godkänna och övervaka genomförandet av riskhanteringsåtgärder för att kunna ställas till svars om de inte efterlevs. Sanktionerna kan innebära att personer i ledande ställning förbjuds att fortsätta utöva sina funktioner. Direktivet kräver också att ledningen genomgår utbildning om riskhanteringsåtgärder och att anställda erbjuds samma utbildning.

Effekter av CER-direktivet

Vissa företag kommer av Sverige att identifieras som ”kritiska entiteter” vilka tillhandahåller samhällsviktiga tjänster inom utpekade sektorer, däribland energi, transport, digital infrastruktur och rymden.

Kritiska entiteter åläggs skyldigheter inbegripet att vidta både tekniska, säkerhetsmässiga och organisatoriska åtgärder för att stärka sin motståndskraft och rapportera incidenter. Som en del av detta ställs krav på systematisk identifikation och bedömning av risker för utpekade hot.

Bland annat ställs krav på fysiskt skydd av lokaler och infrastruktur genom exempelvis förbättrade åtkomstkontroller och övervakningssystem samt en ändamålsenlig hantering av personalsäkerhet.

Ytterligare krav är åtgärder som är nödvändiga för att återhämta sig från incidenter och återuppta tillhandahållet av tjänsten. Som en del av detta kan företag till exempel behöva utveckla och underhålla kontinuitets- och återhämtningsplaner.

Incidenter som medför eller kan medföra en betydande störning i tillhandahållandet av samhällsviktiga tjänster ska rapporteras utan onödigt dröjsmål.

NIS2 kommer att vara tillämpligt för kritiska entiteter enligt CER-direktivet och sådana subjekt kommer därför att behöva efterleva kraven som följer av både CER-direktivet och NIS2.

Förbered verksamheten för att efterleva de nya kraven

Anpassning till nationell lagstiftning

Både NIS2- och CER-direktiven måste införlivas i nationell lagstiftning. För Sverige innebär detta att befintliga cybersäkerhetsregler och föreskrifter måste omarbetas för att säkerställa överensstämmelse med de nya EU-kraven. Sverige ska implementera de krav som ställs i NIS2- och CER-direktiven i nationell rätt, men kan också välja att ställa mer långtgående krav. Företag inom försvar och säkerhet kan därmed inledningsvis förbereda sig på att uppfylla kraven i NIS2- och CER-direktiven. Samtidigt bör företag och branschorganisationer aktivt delta i regelutvecklingsprocessen för att Sverige ska kunna få till ett bra nationellt genomförande och företag bör kontinuerligt övervaka och anpassa sina interna rutiner och processer för att möta de nya nationella kraven på cybersäkerhet och på åtgärder för att stärka motståndskraft som kommer att binda företagen.

Tekniska och organisatoriska förändringar

Genomförandet av NIS2- och CER-direktiven i nationell rätt kommer att innebära att de det ställs krav på såväl tekniska som organisatoriska förändringar inom företagen.

Det innefattar bland annat, men inte uteslutande, att företag kan behöva investera i ny teknologi samt uppdatera befintliga system. Till exempel kan det krävas avancerade säkerhetstekniker såsom intrångsdetekteringssystem, nästa generations brandväggar och krypteringslösningar för att skydda känslig information och kritiska system.

Organisatoriskt krävs det också att företag anpassar sina strukturer och processer för att förbättra sin cybersäkerhet. Detta kan innefatta utveckling och implementering av riskhanteringsstrategier, kontinuerliga säkerhetsutbildningar och simuleringar av cyberattacker för att nå ökad medvetenhet och beredskap. Vidare måste företagen säkerställa att de har tillräckliga resurser och kompetens för att hantera de nya säkerhetskraven. Det är också viktigt att företag etablerar effektiva rapporteringssystem för att snabbt kunna identifiera, hantera och rapportera incidenter.

Översyn av personalsäkerhet och skydd av fysisk miljö

Även systemens fysiska miljö ska skyddas. Det kan innebära att företagen måste införa sträng åtkomstkontroll och se över sin personalsäkerhet och tillgångsförvaltning. Förberedelserna för att anpassa sig till de nya kraven kan innebära behov av att investera i kunskapsfrämjande utbildning för företagets personal, samt att utveckla säkerhetsrutiner som kan stå emot hot.

Dokumentation av åtgärder och förberedelse för tillsyn

Tillsynsmyndigheter kommer att spela en central roll i att säkerställa att företagen följer de nya reglerna, vilket innebär att företag måste vara beredda att dokumentera sina säkerhetsrelaterade åtgärder och processer. För att förbereda sig för tillsynen är det viktigt att företag genomför interna revisioner, säkerhetsövningar och utbildningar. Detta kan öka medvetenheten hos anställda kring sina roller och sitt ansvar inom cybersäkerhet.

Samordning med nationella myndigheter

Företag kan förbereda sig på kommande utökade möjligheter till samverkan med offentliga aktörer och andra privata verksamhetsutövare. Både under NIS2- och CER-direktivet ställs specifika krav på utökad samordning mellan myndigheter och privata verksamhetsutövare. Informationsutbyte är en viktig aspekt för att förebygga, upptäcka, reagera på och återhämta sig från incidenter. Medlemsstaterna förväntas upprätta CISRT-enheter för att snabbt kunna dela information om hot och sårbarheter med privata aktörer. Verksamhetsutövare ska på frivillig basis ges möjlighet att utbyta information om cybersäkerhet sinsemellan.

Slutsats

Sammanfattningsvis är implementeringen av NIS2- och CER-direktiven rättsliga medel för att stärka cybersäkerheten inom försvars- och säkerhetssektorn i Sverige och motståndskraften hos samhällsviktig verksamhet.

Direktiven ska införlivas i nationell rätt och ställer stränga säkerhetskrav och tillsynsåtgärder som företag måste uppfylla för att säkerställa skydd av kritisk infrastruktur och känslig information.

Genom att anpassa sig till dessa nya regelverk, genomföra riskbedömningar och stärka samarbetet med nationella myndigheter, kan svenska företag öka sin resiliens mot cyberhot och bidra till att upprätthålla både nationell och europeisk säkerhet.

Utöver införlivandet av direktivens krav i nationell rätt, kan Sverige välja att ställa mer långtgående krav.

Den svenska lagstiftningsprocessen för nya regler om cybersäkerhet och motståndskraften hos samhällsviktig verksamhet kommer att påverka försvars- och säkerhetssektorn och är därför högst relevant att följa och ta aktiv del i.

NIS2- och CER-direktiven samt tillhörande nationell lagstiftning är dock bara en del av flera initiativ på vägen mot en mer säker digital framtid. Parallellt sker flera politiska satsningar inom till exempel forskning och företagsutveckling och det uppkommer en ökande mängd bidrag att söka för att finansiera omställningen och nyutvecklingen. Framåt finns därför goda skäl att också identifiera och följa dessa typer av satsningar.

Vidare läsning

För att fördjupa er förståelse ytterligare kring NIS2 och CER samt hur dessa påverkar cybersäkerheten i Sverige, rekommenderas följande resurser:

- Europeiska kommissionen: Här hittas offentliga dokument och informations om NIS2-direktivet. Besök https://commission.europa.eu/index_en för att finna specifika dokument och riktlinjer.
- Myndigheten för samhällsskydd och beredskap (MSB): MSB hanterar frågor relaterade till cybersäkerhet i Sverige och har information om hur NIS2 implementeras nationellt. Besök https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/krav-och-regler-inom-informationssakerhet-och-cybersakerhet/nis-direktivet/ för vägledning och ytterligare resurser.
- ENISA (European Union Agency for Cybersecurity): ENISA erbjuder resurser och forskning om olika aspekter av cybersäkerhet, inklusive NIS2-direktivet. Besök https://www.enisa.europa.eu/ för rapporter, vägledningar och verktyg för att stärka cybersäkerhet i Europa.
- EUR-Lex: Alla EU:s förordningar, direktiv och andra rättsakter finns tillgängliga på https://eur-lex.europa.eu/homepage.html?locale=sv.