KÖPINGS KOMMUN

2024-02-21

Säkerhetsavdelningen
Thomas Hoffmann
Säkerhetschef

Nulägesanalys IT-säkerhet Köpings kommun

Inledning
Ledningen ansvarar för informationssäkerhet
Ansvaret för informationssäkerheten är kopplat till det delegerade verksamhetsansvaret. Det betyder att varje person som är ansvarig för en verksamhet också är ansvarig för informationssäkerheten i denna verksamhet. Genom att införa informationssäkerhet i relevanta verksamhetsprocesser åstadkoms en tydlig styrning mot uppsatta mål, ökad kontroll av att fastställda krav uppfylls samt en god informationssäkerhet. För att uppnå god informationssäkerhet krävs att någon arbetar aktivt med området och har ett utpekat ansvar och mandat på central nivå.

Vi utsätts för många cyberhot. Rent allmänt måste vi bli bättre i Sverige på cybersäkerhet. Cyberhoten är ett av de största hoten mot företagen och myndigheterna och det förändras hela tiden med nya motståndare och sårbarheter. Hotet från främmande makt har breddats och blivit mer komplext. Ett flertal länder bedriver i dag olovlig underrättelseverksamhet, spionage, och annan säkerhetshotande verksamhet mot Sverige och svenska intressen. Samtidigt har det säkerhetspolitiska läget i Sveriges närområde allvarligt försämrats. Sveriges överbefälhavare och civilförsvarsminister pekar på att cyberhotet är allvarligt och att åtgärder måste vidtas nu, inte om fem år.

Rättsliga krav på informationssäkerhet i olika verksamheter
Samhällsviktiga tjänster och NIS-regleringen
EU:s NIS-direktiv ställer krav på säkerhet i nätverk och informationssystem. Reglerna omfattar leverantörer av samhällsviktiga tjänster och vissa digitala tjänster. Direktivet införlivas i den svenska rättsordningen genom lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (SFS 2018:1174) och regeringen har beslutat om en förordning (2018:1175) kopplat till den nya lagen. Lagen och förordningen träder i kraft 1 augusti 2018.

Om NIS 2 och CER

Den 14 december 2022 beslutades direktiven om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS 2) och om kritiska entiteters motståndskraft (CER). Direktiven ska börja tillämpas den 18 oktober 2024. Den 23 februari 2023 fattade regeringen beslut om att ge en särskild utredare i uppdrag att föreslå de anpassningar av svensk rätt som är nödvändiga för att NIS 2-direktivet och CER-direktivet ska kunna genomföras. Uppdraget ska redovisas senast 23 februari 2024.

NIS2 i korta drag

EU höjer kraven på företags cybersäkerhet med NIS2-direktivet, som blir svensk lag 2024. Högre krav på rapportering, annars väntar hårda sanktioner. NIS2-direktivet betyder stora förändringar för många företag när direktivet utvidgas och skärps.

Alla samhällsviktiga företag har nu 6 huvudsakliga skyldigheter gällande informationssäkerhet:

- Organisationen har skyldighet att anmäla till tillsynsmyndigheten att de berörs av NIS-regleringen
- Organisationen ska kontinuerligt arbeta strukturerat, metodiskt och riskbaserat med informationssäkerhet enligt vedertagna standardiserade ramverk (ISO 27000-standarden eller motsvarande)
- Årligen analysera verksamhetens risker och upprätta åtgärdsplaner. Dessa ska sedan ligga till grund för val av rätt säkerhetsåtgärder.
- Vidta ändamålsenliga och proportionella åtgärder för att hantera risker som hotar säkerheten
- Vidta lämpliga åtgärder för att förebygga och minimera verkningar av incidenter som påverkar nätverk och informationssystem
- Rapportera incidenter som har en betydande inverkan på den samhällsviktiga tjänsten, tex bortfall eller en störning.

CER-direktivet

CER-direktivet handlar om att säkerställa motståndskraften av samhällsviktig verksamhet. Att förebygga, motstå och hantera störningar eller avbrott i verksamheten inom unionen när det handlar om olyckor, naturkatastrofer, hot mot folkhälsan såsom pandemier och hybridhot. Men även andra hot där det finns en angripare, till exempel vid terroristbrott, brottslig infiltration eller sabotage. I CER-direktivet ingår alltså inte risker kopplade till cybersäkerhet eller hot från cyberattacker utan detta hanteras i NIS2-direktivet.

Dataskyddsförordningen
Alla verksamheter som hanterar personuppgifter måste följa dataskyddsförordningen (GDPR). Det innebär bland annat att vi behöver följa de grundläggande principerna, se till att behandlingen har en rättslig grund och informera de registrerade om hur vi hanterar deras personuppgifter.

Möjliga sanktionsavgifter till följd av dålig lagefterlevnad.

Myndigheter som blir sanktionerade på grund av överträdelser av dataskyddsförordningen drabbas inte lika hårt som privata aktörer. Maxbeloppet som kan drabba myndigheter är inte 20 miljoner euro utan endast 20 miljoner kronor.

Sanktionsavgiften för NIS är som lägst 5 000 kronor och högst 10 000 000 kronor. Avgiften får efterges helt eller delvis under vissa förutsättningar. Leverantörer som omfattas av NIS kan behöva vidta åtgärder för att stärka informationssäkerheten.

Sanktionsavgift för NIS2. För väsentliga entiteter kan avgiften landa på högst 10 MEUR eller 2 % av den globala omsättningen. För viktiga entiteter är sanktionsavgiften högst 7 MEUR eller 1,4 % av den globala omsättningen.

Sammanfattning
IT-säkerhet bör vara ett prioriterat område både utifrån ställda krav men även utifrån ett osäkert omvärldsläge med ökat antal cyberattacker. Köping kommun har genomfört en granskning med hjälp av KPMG utifrån informationssäkerhet som tydligt pekar på stora brister inom området. Säkerhetsavdelningens bedömning är att arbetet måste prioriteras och medel måste avsättas för detta utan dröjsmål.