4 saker som kan hjälpa dig att följa NIS-direktivet

Nyckeln till att arbeta med NIS-direktivet är att ha ett systematiskt och kontinuerligt arbete med informationssäkerhet. Vi har listat fyra saker som kan hjälpa dig att komma igång!

1. Gör en analys

Verkligheten är att alla delar av din organisation inte kan ha det högsta skyddet. Det är därför du måste balansera tillgångar, hot, risker och riskaptit för att hitta rätt åtgärder. I allmänhet är de mest känsliga delarna av en organisation data-överföringar mellan nätverk och domäner.
Du måste bestämma vilken information som är viktigast att skydda. När man arbetar med ett strukturerat, riskbaserat informations-säkerhetsarbete identifierar man information som bör skyddas så att rätt åtgärder kan prioriteras. När du gör en analys kan du överväga följande frågor:
1. Vilka delar är mest kritiska för produktionen?
2. Vilka delar är mest sårbara för attacker?
3. Vilken information är viktigast att skydda?
4. Gör du tillräckligt för att skydda den?
5. Vilken är den rätta skyddsnivån?

2. Skapa en policy

Efter att ha gjort analysen ska målet för organisationens arbete med informationssäkerhet dokumenteras i en policy. Du ska där ha ett strukturerat förhållningssätt för att till exempel klassificera uppgifter, analysera risker och vidta rimliga säkerhetsåtgärder. Du ska också tydliggöra organisationens ansvar för arbetet med informationssäkerhet. Du bör skapa en gedigen incidenthantering för informationen i dessa system och en plan för hur incidenter ska hanteras och hur verksamheten ska gå tillväga efter en incident.

3. Skydda era tillgångar

Efter att ha skapat en policy är det dags att ta reda på hur du behöver skydda din viktigaste information – och till vilken grad. Det är givetvis av stor vikt att de nätverk och informationssystem som används för samhällsviktiga tjänster uppfyller kraven på informationssäkerhet. När de risker som finns har identifierats bör alla resurser som behövs för att kunna utföra arbetet säkerställas och det ska även säkerställas att arbetet anpassas och utvärderas. Det är nu dags att hitta rätt produkter/lösningar för att skydda din information – du kan behöva lösningar för kryptering eller nätverkssegmentering, och kanske på en högre nivå.

4. Arbeta kontinuerligt med informationssäkerhet

Det är viktigt att utbilda medarbetarna och se till att de förstår hur arbetet ska utföras och vad deras roll är. Du bör också se till att implementera en stark säkerhetskultur. Du ska även ha en gedigen incidenthantering för informationen i dina system och en plan för hur incidenter ska hanteras och hur verksamheten ska gå tillväga efter en incident. Du bör arbeta strukturerat och metodiskt med informationssäkerhet enligt vedertagna standardiserade ramverk (standard ISO 27000 eller motsvarande).

Advenica tillhandahåller expertis, hög assurans och cybersäkerhetslösningar i världsklass för kritisk data-in-motion upp till Top Secret-klassning. Med oss stärker länder, myndigheter och företag informationssäkerheten och digitaliserar ansvarsfullt. Bolaget grundades 1993 och har EU-godkännande på högsta säkerhetsnivå. Våra unika produkter designas, utvecklas och tillverkas i Sverige.

Läs mer på advenica.com

advenica

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED