Omfattas ni av NIS-2? Då är det hör tid att se över var på kartan ni befinner er i ert arbete. Fundera över om ni kan använda er av några redan befintliga standars eller ramverk eller om ni behöver plocka in nya.

Identifiera Tillämplighet:

NIS: Omfattade operatörer av väsentliga tjänster (OES) och digitala tjänsteleverantörer (DSP).

NIS-2: Utökar tillämpningsområdet till att inkludera fler sektorer och typer av organisationer, även medelstora och små företag inom kritiska sektorer.

Riskbedömning och Säkerhetspolicys:

Genomför en detaljerad riskbedömning med hänsyn till de utökade kraven i NIS-2.

Uppdatera eller utveckla säkerhetspolicys och procedurer som återspeglar NIS-2:s förstärkta krav.

Incidenthantering:

NIS: Krävde rapportering av incidenter som hade en betydande inverkan.

NIS-2: Inför striktare krav på rapportering av incidenter, med kortare tidsfrister för att anmäla incidenter till relevanta myndigheter.

Säkerhetsåtgärder och System härdning:

Implementera avancerade säkerhetsåtgärder som adresserar de identifierade riskerna, inklusive systemhärdning, regelbunden uppdatering av programvara och hårdvara, samt stark autentisering och åtkomstkontroll.

Övervakning och Detektion:

Förbättra kapaciteten för övervakning och detektion av cyberhot och incidenter.

Utbildning och Medvetenhet:

Utbilda anställda och intressenter om NIS-2:s krav och bästa praxis för cybersäkerhet.

Testning och Övningar:

Genomför regelbundna säkerhetstestningar och övningar för att verifiera effektiviteten av säkerhetsåtgärderna och incidenthanteringsprocedurerna.

Leverantörskedjans Säkerhet:

NIS-2: Inför krav på säkerhet i leverantörskedjan, vilket kräver att organisationer säkerställer att deras leverantörer och underleverantörer också uppfyller lämpliga säkerhetsstandarder.

Rapportering och Kommunikation:

Etablera och underhåll kommunikationskanaler för effektiv rapportering och samarbete med nationella cybersäkerhetsmyndigheter och andra relevanta organ.

Dokumentation och Efterlevnadsbevis:

Dokumentera alla säkerhetsåtgärder och procedurer för att kunna uppvisa efterlevnad vid revisioner och inspektioner.

Översyn och Kontinuerlig Förbättring:

Inför en **process** för **kontinuerlig** översyn och förbättring av cybersäkerhetspraxis i enlighet med NIS-2:s dynamiska natur och det ständigt föränderliga cybersäkerhetslandskapet.

Viktiga Skillnader Från NIS

Tillämpningsområde: NIS-2 har ett betydligt bredare tillämpningsområde, inkluderande fler sektorer och även mindre organisationer inom vissa kritiska sektorer.

Rapporteringskrav: Striktare och mer detaljerade krav på rapportering av säkerhetsincidenter.

Leverantörskedjans Säkerhet: Nya krav