SECURANCE

Step-by-step Guide -

NIS2 (Network and Information Security Directive 2).

Introductie

De Netwerk- en Informatiesystemen Richtlijn 2 (NIS2) is een cruciale verordening van de Europese Unie gericht op het versterken van de cyberveiligheid en veerkracht van kritieke infrastructuur in verschillende sectoren. Als opvolger van de oorspronkelijke NIS-richtlijn introduceert NIS2 strengere eisen en een uitgebreidere dekking om de beveiliging en continuïteit van essentiële en belangrijke entiteiten binnen het digitale landschap te verbeteren. Naleving van NIS2 is zowel een wettelijk mandaat als een essentiële strategie voor organisaties om hun activiteiten te beschermen tegen een zich ontwikkelende reeks cyberbedreigingen en verstoringen.

Deze handleiding biedt een uitgebreide stapsgewijze aanpak voor het implementeren van NIS2 binnen uw organisatie. We beginnen met de verklaring van toepasselijkheid, waarin de specifieke NIS2-vereisten voor uw organisatie worden beschreven. Vervolgens voeren we een GAP-analyse uit om vast te stellen waar uw bestaande cyberbeveiligingspraktijken tekortschieten ten opzichte van de NIS2-standaarden. Op basis van deze analyse ontwikkelen we een plan om de geconstateerde tekortkomingen te verhelpen. Voor lacunes met een gemiddelde of lage prioriteit voeren we een gedetailleerde risicoanalyse uit om effectieve risicobeperkende strategieën te formuleren. Tot slot gaan we over naar de implementatiefase, waarin we de noodzakelijke maatregelen uitvoeren om naleving te garanderen. Door deze stappen te volgen, kan uw organisatie niet alleen voldoen aan de NIS2-vereisten, maar ook haar algehele weerbaarheid tegen cyberbedreigingen en -uitdagingen versterken.

NIS2

Het primaire doel van de NIS2 is het verbeteren van de cyberbeveiliging en operationele weerbaarheid van essentiële en belangrijke entiteiten in verschillende sectoren. Deze verordening schrijft voor dat organisaties robuuste maatregelen implementeren om de risico's van netwerk- en informatiesystemen te beheren en te beperken, zodat ze effectief kunnen reageren op en herstellen van cyberincidenten. NIS2 breidt de vereisten uit naar een breder scala van sectoren en entiteiten en benadrukt de noodzaak van uitgebreide cyberbeveiligingspraktijken en incidentbeheer.

De Kern van NIS2 Componenten bestaat uit:

- **Cybersecurity Risk Management:** Organisaties moeten uitgebreide risicobeheersystemen voor cyberbeveiliging opzetten en onderhouden. Dit houdt in dat risico's met betrekking tot netwerk- en informatiesystemen worden geïdentificeerd, beoordeeld en beperkt. Effectief risicobeheer omvat het hebben van een up-to-date inventaris van bedrijfsmiddelen, het beoordelen van potentiële bedreigingen en het implementeren van maatregelen om bescherming te bieden tegen geïdentificeerde risico's.

- **Incident Reporting:** NIS2 bepaalt dat entiteiten gestandaardiseerde procedures moeten ontwikkelen voor het melden van significante cyberbeveiligingsincidenten aan nationale autoriteiten. Dit voorschrift bevordert transparantie, vergemakkelijkt snelle reacties en ondersteunt gecoördineerde inspanningen tussen verschillende belanghebbenden om de impact van cyberdreigingen aan te pakken en te beperken.

- **Resilience Testing:** Entiteiten moeten hun cyberbeveiligingsmaatregelen en -systemen regelmatig testen om kwetsbaarheden te identificeren en aan te pakken. Dit omvat het uitvoeren van kwetsbaarheidsbeoordelingen, penetratietests en andere beveiligingsoefeningen om de robuustheid van hun verdediging te garanderen.

- **Supply Chain Security:** NIS2 erkent de cruciale rol van externe leveranciers en schrijft voor dat organisaties hun toeleveringsketens effectief moeten beheren en beveiligen. Dit houdt in dat er maatregelen moeten worden genomen om de cyberbeveiligingspraktijken van externe partners te beoordelen en te controleren en dat er contractuele afspraken moeten worden gemaakt over cyberbeveiligingsrisico's en verantwoordelijkheden.

- **Operational Continuity:** Organisaties moeten plannen ontwikkelen en onderhouden om de continuïteit van hun essentiële diensten te garanderen, zelfs in het geval van aanzienlijke verstoringen. Dit omvat het maken en testen van rampherstelplannen en bedrijfscontinuïteitsprocedures om veerkracht te garanderen in het geval van een groot incident.

Door te voldoen aan de vereisten van NIS2 kunnen organisaties hun vermogen om risico's voor cyberbeveiliging te beheren aanzienlijk verbeteren en de continuïteit van hun activiteiten waarborgen. NIS2 bevordert een proactieve benadering van cyberbeveiliging en stimuleert voortdurende verbetering en samenwerking tussen entiteiten, waardoor de algehele beveiliging en veerkracht van kritieke sectoren wordt versterkt.

Fase 1. Fit-Gap analysis level 1 en level 2

Bepalen welke specifieke aspecten van NIS2 van toepassing zijn op de organisatie

Door een grondige STAP-analyse (Statement of Applicability) uit te voeren, kan de organisatie duidelijk begrijpen welke NIS2-vereisten relevant zijn voor haar activiteiten en bepalen op welke gebieden ze voldoet (FIT) en niet voldoet (GAP). Deze analyse vormt de basis voor de volgende stappen in het nalevingsproject en zorgt voor een gerichte en efficiënte aanpak om volledige naleving van NIS2 te bereiken.

- **Bestaande compliance documenteren**
  Een eerste beoordeling uitvoeren van de maatregelen, beleidslijnen en procedures van de organisatie op het gebied van cyberbeveiliging. Identificeer en documenteer gebieden waarop de organisatie al voldoet aan de NIS2-eisen, waaronder bestaande risicobeheerpraktijken, meldingsmechanismen voor incidenten en beveiligingscontroles.

- **Identificeer en documenter GAPS**
  Een gedetailleerd overzicht maken van de NIS2-vereisten en deze vergelijken met de huidige status van de organisatie. Identificeer en documenteer gebieden waarop de organisatie niet voldoet aan de NIS2-eisen. Hierbij kan het gaan om ontbrekende beleidsregels, ontoereikende controles of verouderde procedures.

- **Evalueer impact and waarschijnlijkheid**
  Evalueer de prioriteit van elk geïdentificeerd hiaat op basis van de potentiële impact op de organisatie en de waarschijnlijkheid van uitbuiting. Overweeg het kritieke karakter van de getroffen systemen en processen en de mogelijke gevolgen van niet-naleving. Verdeel de hiaten in hiaten met lage, gemiddelde en hoge prioriteit.

- **Houd gesprekken met stakeholders**
  Interviews houden met de belangrijkste belanghebbenden op verschillende afdelingen om gedetailleerde inzichten te verzamelen in de huidige praktijken en om de geïdentificeerde hiaten te valideren. Samenwerken met IT-, beveiligings-, compliance- en operationele teams om een uitgebreide dekking van alle relevante gebieden te garanderen.

- **Beoordeel en valideer**
  Voer een interne review uit van het STAP-analyserapport met het projectteam en het senior management om de nauwkeurigheid en volledigheid ervan te garanderen. Valideer de bevindingen met relevante belanghebbenden om te zorgen voor afstemming en buy-in.

- **Rapport en feedback**
  Een rapport met een samenvatting van de bevindingen van de FitGap-analyse zal worden samengesteld met een gedetailleerde beschrijving van de geïdentificeerde hiaten en de huidige versus de gewenste staat voor elk. De bevindingen zullen worden gepresenteerd aan relevante belanghebbenden en er zal feedback worden verzameld om de analyse te verfijnen.

Fase 2. Gap Closure Plan

Een uitgebreid plan ontwikkelen om de vastgestelde hiaten aan te pakken en te voldoen aan de NIS2

In deze stap worden specifieke acties beschreven voor hiaten met een hoge prioriteit en worden middelen toegewezen om ervoor te zorgen dat effectief aan alle compliancevereisten wordt voldaan.

Het Gap Closure Plan omvat het volgende:

- **Analyse van zowel de huidige als gewenste situatie**
  Voor elke vastgestelde lacune wordt de bestaande toestand van beveiligingsmaatregelen en -praktijken beschreven, evenals de gewenste situatie. Dit omvat een gedetailleerde beschrijving van de specifieke tekortkomingen, hoe deze tekortschieten ten opzichte van de vereisten voor NIS2 en duidelijke, meetbare doelstellingen waarmee de vastgestelde hiaten worden aangepakt.

- **Definieer specifieke acties en metingen**
  Voor elk geïdentificeerd hiaat worden de acties gespecificeerd die nodig zijn om het hiaat te overbruggen. De details omvatten wat er gedaan moet worden, wie er verantwoordelijk is en welke middelen nodig zijn.

- **Bepaal prioriteiten en timeline**
  De hiaten met een hoge prioriteit zullen opnieuw worden geprioriteerd op basis van risiconiveau, impact en urgentie. Ook zal er voor elke actie een realistisch tijdschema worden ontwikkeld, waarbij rekening wordt gehouden met de complexiteit van de taken en de beschikbaarheid van middelen.

- **Voorbereiding van implementatie**
  Er worden uitgebreide plannen ontwikkeld met de stappen die nodig zijn om elke herstelactie uit te voeren. Dit omvat het opstellen van alle benodigde documentatie, trainingsmaterialen en communicatieplannen.

- **Documenteer en rapporteer**

Er zal een rapport worden geleverd met een samenvatting van de analyse, gedefinieerde acties, prioriteiten, tijdschema's en voorbereidingen voor de implementatie. Het rapport zal worden voorgelegd aan relevante belanghebbenden en staat open voor feedback om ervoor te zorgen dat alle perspectieven in aanmerking worden genomen. Potentiële eerste stappen om de implementatie van de acties in het gap closure plan op te starten zullen worden opgenomen.

Door deze stappen te volgen, kan de organisatie zorgen voor een systematische en effectieve aanpak om vastgestelde hiaten te dichten en naleving van NIS2 te bereiken.

Fase 3. Risicoanalyse voor GAP's met gemiddelde en lage prioriteit

De risico's in verband met de geïdentificeerde hiaten beoordelen en acties prioriteren

In deze stap wordt een grondige risicobeoordeling uitgevoerd om inzicht te krijgen in de potentiële bedreigingen en kwetsbaarheden van de geïdentificeerde kloof met lage en gemiddelde prioriteit.

Acties:

- **Risicoanalyse uitvoeren**
  De ernst van elk risico zal worden beoordeeld door zowel de potentiële impact op de organisatie als de waarschijnlijkheid dat het zich voordoet in overweging te nemen. Er zullen kwalitatieve en kwantitatieve methoden worden gebruikt om deze risico's te evalueren.

- **Bepaal impact en waarschijnlijkheid**
  De mogelijke gevolgen van elk risico voor de organisatie worden bepaald. Risico's met een grote impact zijn bijvoorbeeld aanzienlijke financiële verliezen, ernstige reputatieschade, boetes van regelgevende instanties of grote operationele verstoringen.

  De waarschijnlijkheid dat elk risico zich voordoet, zal worden geëvalueerd. Factoren die de waarschijnlijkheid beïnvloeden zijn bijvoorbeeld de huidige controles van de organisatie, historische incidenten, trends in de sector en de kwetsbaarheid voor specifieke bedreigingen.

- **Creeer een Risicomatrix**
  Er wordt een risicomatrix ontwikkeld waarin de waarschijnlijkheid van elk risico wordt afgezet tegen de potentiële impact. Dit visuele hulpmiddel helpt bij het categoriseren van risico's in verschillende niveaus van ernst. Op basis van de matrix wordt elk risico ingedeeld in de juiste niveaus. Risico's met een hoge impact en een hoge waarschijnlijkheid krijgen prioriteit als kritiek, terwijl risico's met een lagere impact en een lagere waarschijnlijkheid kunnen worden gecategoriseerd als lage prioriteit.

- **Ontwikkel een lijst met prioriteiten**
  Er zal een geprioriteerde lijst van risico's op basis van hun ernstniveaus uit de risicomatrix worden ontwikkeld. De focus zal liggen op het eerst aanpakken van de meest kritieke risico's om de grootste potentiële impact op de organisatie te beperken.

- **Actieplanning**
  Voor elk geprioriteerd risico worden specifieke acties en maatregelen geschetst. Dit kan bestaan uit het verbeteren van beveiligingscontroles, het bijwerken van beleidsregels, het implementeren van nieuwe technologieën of het geven van aanvullende training.

- **Ontwikkel een timeline**
  Er zullen realistische tijdschema's worden opgesteld voor het implementeren van de risicobeperkende acties. Acties die kritieke risico's met de grootste impact en waarschijnlijkheid aanpakken, krijgen prioriteit.

- **Documentatie en rapportage**
  Alle risicobeoordelingen worden gedetailleerd bijgehouden, inclusief de redenen voor de impact- en waarschijnlijkheidsbeoordelingen en de prioriteringsbeslissingen.

Door deze stappen te volgen, kan de organisatie de risico's die gepaard gaan met de geïdentificeerde hiaten effectief beoordelen en prioriteren, en ervoor zorgen dat de middelen worden gericht op de meest kritieke gebieden.

Fase 4. Implementatie

Implementeren van de acties

Deze stap zorgt ervoor dat middelen efficiënt worden toegewezen, waarbij de aandacht eerst uitgaat naar de meest kritieke gebieden om belangrijke risico's te beperken.

Acties:

- **Uitvoering van GAP-closure plan**
  De specifieke acties om de hiaten aan te pakken die tijdens de FitGap Analyse zijn geïdentificeerd, zullen worden geïmplementeerd. Deze acties kunnen bestaan uit het bijwerken van beleid en procedures, het verbeteren van de technologische infrastructuur, het implementeren van nieuwe beveiligingsmaatregelen of het verbeteren van operationele processen.

- **Communiceren van beleids- en proceswijzigingen**
  Veranderingen in beleid, procedures of praktijken worden gecommuniceerd met relevante belanghebbenden binnen de organisatie. Dit zorgt ervoor dat iedereen zijn rol en verantwoordelijkheden begrijpt met betrekking tot de naleving van de NIS2-vereisten.

- **Testen en validatie**
  NIS2-compliancemaatregelen omvatten meestal het testen van systemen en processen om ervoor te zorgen dat ze werken zoals bedoeld.

- **Monitoring en rapportage**
  Er zullen mechanismen worden vastgesteld om toezicht te houden op de voortdurende naleving van de NIS2-eisen. Dit kan inhouden dat er regelmatige audits, beoordelingen of systemen voor continue monitoring worden opgezet om afwijkingen of problemen snel op te sporen en aan te pakken.

- **Documentatie en rapportage**
  Er wordt een uitgebreide documentatie bijgehouden van alle geïmplementeerde maatregelen, wijzigingen en nalevingsactiviteiten. Deze documentatie is essentieel om naleving aan te tonen tijdens audits of vragen van regelgevende instanties.

- **Evaluatie en voortdurende verbeteringen**
  De geïmplementeerde maatregelen zullen periodiek worden geëvalueerd om hun effectiviteit te beoordelen en gebieden voor verbetering te identificeren. Continue verbetering zorgt ervoor dat de organisatie na verloop van tijd bestand blijft tegen digitale operationele risico's.

- **Aanpassing aan veranderende eisen**
  Gezien de dynamische aard van de wettelijke vereisten, moeten we op de hoogte blijven van wijzigingen of updates van NIS2 en het implementatieplan dienovereenkomstig aanpassen.

Door een gestructureerde implementatieaanpak te volgen, kunnen organisaties hun cyberbeveiligingspositie verbeteren en effectief voldoen aan de NIS2-vereisten.

Maak kennis met Securance

Investeer in efficiëntie, waarde, en partnerschap

- **Analyseer risico's**
- **Plan het project**
- **Bereid systeembeschrijvingen voor**
- **Voer een gereedheidsbeoordeling uit**

Het voldoen aan NIS2 wetgeving vereist zorgvuldige planning, betrokken leiderschap, een grondige analyse van processen en betrouwbare middelen en projectmanagement.

Securance is voortgekomen uit een 'Big Four'-accountantskantoor en werd opgericht in 2004. Dankzij onze achtergrond werken wij volgens de hoogste professionele standaarden en hebben wij ervaring met het behalen van strakke deadlines. Wij hanteren deze professionele standaarden in al ons werk en leveren altijd de hoogste kwaliteit, terwijl we continu streven naar het voldoen aan de behoeften van onze klanten.

Door onze platte organisatiestructuur en efficiënte communicatielijnen kunnen wij snel inspelen op uw wensen. Kiezen voor Securance betekent kiezen voor een professionele organisatie, maar ook voor een persoonlijke aanpak. Effectief projectmanagement, onze ervaring met het implementeren van risicobeheersingskaders binnen uw sector en onze professionaliteit vormen volgens ons de basis voor uitstekende resultaten.

Bij Securance geloven wij dat een goed begrip van uw organisatie, heldere communicatie en diepgaande kennis van uw sector essentieel zijn om u als klant meerwaarde te bieden. Op basis van deze aanpak houden wij u op de hoogte van relevante wetswijzigingen, regelgeving en andere belangrijke ontwikkelingen.

SECURANCE
BE SURE

Onze tevreden klanten

Referenties

BECOME THE ARCHITECT OF YOUR FUTURE

Neem contact met ons op

SECURANCE

Securance Ltd.

63-66 Hatton Garden

London EC1N 8LE, UK

+44 20 351 446 56

www.securance.co.uk

Securance BV

Reactorweg 47

3542 AD Utrecht

+31 (0)30 2800888

www.securance.nl