Van: info@teamx24.com <info@teamx24.com>
Verzonden: dinsdag 9 juli 2024 11:05
Aan: Gemeenteraad

Onderwerp: Uitleg over NIS2-richtlijn en de rol van de gemeenteraad, burgemeester, gemeentesecretaris

Geachte leden van de gemeenteraad, burgemeester, gemeentesecretaris,

Met deze brief willen wij uw aandacht vestigen op de NIS2-richtlijn en de cruciale rol die de gemeenteraad speelt in de implementatie en borging van deze richtlijn binnen onze gemeente. Bijgevoegd vindt u het "Handboek voor het inrichten van de NIS2-Richtlijn bij de Gemeente", dat gedetailleerde handvatten biedt voor de implementatie van deze richtlijn.

Wat is NIS2?

De NIS2-richtlijn (Netwerk- en Informatiebeveiliging 2) is een Europese regelgeving die gericht is op het verhogen van de beveiliging van netwerk- en informatiesystemen binnen de EU-lidstaten. Deze richtlijn legt nadruk op het vergroten van de weerbaarheid van essentiële en belangrijke entiteiten tegen cyberdreigingen en andere digitale risico's.

Uw rol als gemeenteraad

Als gemeenteraad hebt u de verantwoordelijkheid om ervoor te zorgen dat onze gemeente voldoet aan de eisen van de NIS2-richtlijn. Dit omvat niet alleen de initiële implementatie van beveiligingsmaatregelen, maar ook het continu onderhouden en verbeteren van deze maatregelen om te voldoen aan de steeds veranderende dreigingen.

Wij, als experts van het NIS2ok-initiatief onder TeamX24 B.V., geleid door mijzelf, Dr. Mohamad Adib Baroud, NIS2-expert, staan klaar om u te ondersteunen bij dit proces. We willen u graag de volgende stappen voorstellen:

1. Uitleg komen geven hoe de NIS2 in het gemeentelijk aparat inbedden. (zie bijlage)
2. Begeleiding en status in Initiële Implementatie:

- Risicoanalyse en Beoordeling: Identificeren van kritieke systemen en mogelijke kwetsbaarheden.
- Beveiligingsmaatregelen: Implementeren van basisbeveiligingsmaatregelen volgens de NIS2-richtlijn.

3. Richten, Inrichten en Verrichten van Continuïteit:

- Richten: Strategische doelen stellen voor cyberbeveiliging binnen de gemeente.
- Inrichten: Opzetten van een organisatiebreed beleid en toewijzen van verantwoordelijkheden.
- Verrichten: Continu monitoren, evalueren en verbeteren van beveiligingsmaatregelen.

4. Bewustwording en Training:

- Opleiding van alle stakeholders: Regelmatige training en bewustwordingscampagnes voor iedereen om hen op de hoogte te houden van de nieuwste dreigingen en beveiligingsmaatregelen.
- Incidentenbeheer: Opstellen en testen van een incidentenresponsplan om snel en effectief te reageren op beveiligingsincidenten.

Onze Aanbieding

Wij nodigen u uit voor een uitgebreide presentatie waarin we gedetailleerd ingaan op de NIS2-richtlijn en de specifieke stappen die uw gemeente moet nemen om compliant te zijn. Tijdens deze sessie kunnen we ook uw vragen beantwoorden en specifieke aandachtspunten voor uw gemeente bespreken.

Afsluiting

Wij geloven dat een proactieve en goed geïnformeerde aanpak essentieel is om de beveiliging van onze gemeentelijke systemen te waarborgen. Uw betrokkenheid en inzet zijn cruciaal voor het succes van deze onderneming.

Bijgevoegd vindt u het "Handboek voor het inrichten van de NIS2-Richtlijn bij de Gemeente", dat gedetailleerde handvatten biedt voor de implementatie van deze richtlijn.

We kijken ernaar uit om samen te werken aan een veilige en veerkrachtige digitale omgeving voor onze gemeente.

Met vriendelijke groet,

Dr. Mohamad Adib Baroud
NIS2-expert
TeamX24 B.V.
NIS2ok Initiatief
info@teamx24.nl
06-geanonimiseerd

Handboek voor het inrichten van de NIS2-Richtlijn bij de Gemeente

Dit handboek geeft handvatten van hoe te werk gaan bij de gedeelde taken die bij een gemeente horen. De Gemeenteraad is dan de baas over de gemeente maar moeten volgens afgesproken structuur verlopen.

Contents

Verantwoordelijkheid van Gemeenteraad, Burgemeester, Gemeentesecretaris/Algemeen Directeur

In het kader van de NIS2-richtlijn en de verantwoordelijkheden van de gemeentelijke overheid voor cyberbeveiliging, zijn de rollen en verantwoordelijkheden als volgt verdeeld:

Verantwoordelijkheid en Aansprakelijkheid

Gemeenteraad:

- De gemeenteraad is het hoogste bestuursorgaan van de gemeente en stelt het algemene beleid vast. De raad heeft de verantwoordelijkheid om ervoor te zorgen dat er een adequaat beleid voor cyberbeveiliging is, inclusief de naleving van de NIS2-richtlijn.

Burgemeester:

- De burgemeester heeft een belangrijke rol in de handhaving van de openbare orde en veiligheid, inclusief digitale veiligheid. De burgemeester kan worden gezien als de uitvoerder van het beleid dat door de gemeenteraad is vastgesteld. Bij incidenten of crises kan de burgemeester snel maatregelen nemen.

Gemeentesecretaris/Algemeen Directeur:

- De gemeentesecretaris (ook wel de algemeen directeur genoemd) is verantwoordelijk voor de dagelijkse leiding van de ambtelijke organisatie. Deze persoon zorgt ervoor dat het beleid, inclusief maatregelen voor cyberbeveiliging en naleving van de NIS2-richtlijn, daadwerkelijk wordt geïmplementeerd en uitgevoerd.

Aansprakelijkheid bij Nieuwe Verkiezingen

Wanneer er nieuwe verkiezingen zijn, kan de verantwoordelijkheid en aansprakelijkheid voor de naleving van de NIS2-richtlijn als volgt worden beschouwd:

1. Gemeenteraad: Blijft als orgaan verantwoordelijk voor het vaststellen van het beleid, ongeacht wie er zitting heeft. De nieuwe raad neemt de verantwoordelijkheid over van de vorige raad.

2. Burgemeester: Blijft verantwoordelijk voor de uitvoering van het beleid en de handhaving van de openbare orde en veiligheid, inclusief digitale veiligheid, totdat een nieuwe burgemeester wordt benoemd. De burgemeester heeft een continue verantwoordelijkheid.

3. Gemeentesecretaris/Algemeen Directeur: Blijft verantwoordelijk voor de operationele uitvoering van het beleid, inclusief de maatregelen voor cyberbeveiliging. Deze rol is doorgaans niet direct afhankelijk van verkiezingen, omdat de gemeentesecretaris een ambtelijke functie bekleedt.

Gedeelde Aansprakelijkheid

In de praktijk is de verantwoordelijkheid voor naleving van de NIS2-richtlijn vaak gedeeld:

- Strategische Verantwoordelijkheid: De gemeenteraad en burgemeester delen de strategische verantwoordelijkheid voor het vaststellen en handhaven van het beleid.

- Tactische Verantwoordelijkheid: De burgemeester en gemeentesecretaris zijn verantwoordelijk voor de tactische uitvoering van het beleid.

- Operationele Verantwoordelijkheid: De gemeentesecretaris zorgt voor de operationele uitvoering en naleving van het beleid door de ambtelijke organisatie.

Door deze stappen te volgen, kan de gemeente de naleving van de NIS2-richtlijn waarborgen en de digitale weerbaarheid versterken.

Advies

Voor de gemeente is het cruciaal om een duidelijke governance-structuur te hebben waarbij de verantwoordelijkheden en bevoegdheden voor cyberbeveiliging en naleving van de NIS2-richtlijn expliciet zijn vastgelegd. Dit helpt niet alleen bij de continuïteit tijdens verkiezingen, maar zorgt er ook voor dat er altijd duidelijkheid is over wie verantwoordelijk is voor welke aspecten van cyberbeveiliging.

Daarnaast is het belangrijk om regelmatig te evalueren en rapporteren over de naleving van de NIS2-richtlijn en de algehele cyberbeveiligingsstatus. Dit zorgt ervoor dat de gemeenteraad, de burgemeester en de gemeentesecretaris allemaal goed geïnformeerd zijn en dat de gemeente als geheel 'in control' is.

Bob-sessie over Bewustwording van de NIS2 op Strategisch, Tactisch en Operationeel Niveau voor de Gemeenteraad

1. Inleiding

Doel van de sessie:

Het doel van deze BOB-sessie is om de gemeenteraad bewust te maken van de NIS2-richtlijn en de implicaties ervan op strategisch, tactisch en operationeel niveau. Tevens zullen we bespreken welke vragen aan het college van Burgemeester en Wethouders (B&W) gesteld moeten worden om te verzekeren dat de gemeente in control is.

2. Beeldvorming (B)

Strategisch Niveau:

- Wat is de NIS2-richtlijn?

- De NIS2-richtlijn is een Europese regelgeving die de beveiliging van netwerk- en informatiesystemen van essentiële en belangrijke diensten versterkt.

- Waarom is de NIS2-richtlijn belangrijk voor de gemeente?

- De richtlijn verplicht gemeenten om maatregelen te nemen om hun netwerk- en informatiesystemen tegen incidenten te beschermen, wat cruciaal is voor de continuïteit van gemeentelijke diensten.

- Wat zijn de gevolgen van niet-naleving?

- Niet-naleving kan leiden tot boetes, reputatieschade en verhoogde kwetsbaarheid voor cyberaanvallen.

Tactisch Niveau:

- Welke systemen en processen vallen onder de NIS2?

- Alle kritieke IT-systemen en processen die essentieel zijn voor de dienstverlening van de gemeente.

- Hoe wordt de naleving van de NIS2 gemeten en gecontroleerd?

- Door regelmatige audits, risicobeoordelingen en nalevingsrapporten.

- Welke rol spelen verschillende afdelingen in de naleving?

- IT, juridische zaken, HR en de afdelingen die verantwoordelijk zijn voor de levering van essentiële diensten.

Operationeel Niveau:

- Wat zijn de dagelijkse implicaties voor gemeentelijke medewerkers?

- Medewerkers moeten zich houden aan strikte beveiligingsprotocollen, zoals wachtwoordbeheer en meldingsprocedures voor incidenten.

- Welke technische maatregelen moeten worden geïmplementeerd?

- Multifactor authenticatie, regelmatige software-updates, en versleuteling van gegevens.

- Hoe worden incidenten gedetecteerd en gemeld?

- Door middel van monitoringtools en een duidelijk incidentresponsplan.

3. Oordeelsvorming (O)

Strategisch Niveau:

- Hoe past de NIS2 in de bredere strategie van de gemeente voor digitale transformatie?

- NIS2 moet worden gezien als een essentieel onderdeel van de digitale transformatie en risicobeheerstrategie.

- Welke middelen en budget zijn nodig voor NIS2-naleving?

- Inzicht in de benodigde middelen voor technologie, personeel en training.

Tactisch Niveau:

- Hoe zorgt de gemeente voor voortdurende naleving van de NIS2?

- Door het instellen van een compliance officer en het regelmatig herzien van beveiligingsmaatregelen.

- Wat zijn de belangrijkste risico's die de gemeente moet beheren?

- Identificatie van de meest kritieke risico's en de ontwikkeling van plannen om deze te mitigeren.

Operationeel Niveau:

- Hoe wordt de training en bewustwording van medewerkers gewaarborgd?

- Regelmatige trainingssessies en bewustwordingscampagnes.

- Welke procedures zijn er voor incidentrespons en herstel?

- Een gedetailleerd incidentresponsplan en regelmatige oefeningen om de paraatheid te testen.

4. Besluitvorming (B)

Voorstellen en Amendementen:

1. Voorstel: Instellen van een NIS2-coördinator binnen de gemeente die verantwoordelijk is voor de naleving van de richtlijn.

- Amendement: De NIS2-coördinator rapporteert rechtstreeks aan de gemeentesecretaris en presenteert kwartaalrapporten aan de raad.

2. Voorstel: Ontwikkelen van een jaarlijks auditprogramma om de naleving van de NIS2-richtlijn te waarborgen.

- Amendement: De resultaten van de audits worden gedeeld met alle relevante afdelingen en besproken in een jaarlijkse veiligheidsreview.

3. Voorstel: Implementeren van een continu trainingsprogramma voor alle gemeentemedewerkers over cyberbeveiliging en NIS2-naleving.

- Amendement: Trainingen moeten ten minste halfjaarlijks plaatsvinden en er moet een certificeringsproces worden opgezet om de voltooiing te bevestigen.

5. Vragen aan het College van B&W

Strategisch Niveau:

1. Hoe integreert de gemeente de naleving van de NIS2-richtlijn in haar bredere digitale strategie?

2. Welke stappen zijn er genomen om de strategische risico's van cyberaanvallen te verminderen?

Tactisch Niveau:

1. Welke afdelingen en functies zijn verantwoordelijk voor de naleving van de NIS2-richtlijn?

2. Hoe vaak worden risicobeoordelingen en nalevingsaudits uitgevoerd?

Operationeel Niveau:

1. Hoe worden gemeentelijke medewerkers getraind in de vereisten en procedures van de NIS2-richtlijn?

2. Wat zijn de protocollen voor het melden en afhandelen van beveiligingsincidenten?

6. Conclusie

Samenvatting:

Het is cruciaal dat de gemeente een uitgebreide strategie en gedetailleerde procedures implementeert om aan de NIS2-richtlijn te voldoen. Door het stellen van de juiste vragen en het implementeren van duidelijke voorstellen en amendementen, kan de gemeenteraad ervoor zorgen dat de gemeente goed voorbereid is op de uitdagingen van cyberbeveiliging en continuïteit van dienstverlening.

Actiepunten:

- Aanstellen van een NIS2-coördinator.

- Ontwikkelen en implementeren van een auditprogramma.

- Opzetten van een continu trainingsprogramma.

Governance-structuur voor Naleving van de NIS2-Richtlijn in een Gemeente

1. Gemeenteraad

Rol:

- Vaststellen van het strategische beleid voor cyberbeveiliging en naleving van de NIS2-richtlijn.

- Toezicht houden op de uitvoering van het beleid door de burgemeester en gemeentesecretaris.

Verantwoordelijkheden:

- Goedkeuren van budgetten en middelen voor cyberbeveiligingsinitiatieven.

- Evalueren van jaarlijkse rapporten over de staat van cyberbeveiliging en naleving van de NIS2-richtlijn.

- Ingrijpen bij ernstige incidenten of niet-naleving door aanvullende maatregelen te eisen.

2. Burgemeester

Rol:

- Handhaving van het vastgestelde beleid en coördinatie van de strategische en tactische respons bij cyberincidenten.

- Vertegenwoordigen van de gemeente bij regionale en nationale cyberbeveiligingsinitiatieven.

Verantwoordelijkheden:

- Leiding geven aan de uitvoering van het cyberbeveiligingsbeleid.

- Samenwerken met de gemeentesecretaris om de implementatie van maatregelen te waarborgen.

- Rapporteren aan de gemeenteraad over de voortgang en eventuele problemen met betrekking tot cyberbeveiliging.

3. Gemeentesecretaris (Algemeen Directeur)

Rol:

- Dagelijkse leiding over de ambtelijke organisatie en operationele uitvoering van het cyberbeveiligingsbeleid.

- Fungeren als schakel tussen het strategische beleid van de gemeenteraad en de operationele uitvoering.

Verantwoordelijkheden:

- Implementeren van de vastgestelde cyberbeveiligingsmaatregelen en naleving van de NIS2-richtlijn.

- Toezicht houden op de ICT-afdeling en het Information Security Management Team (ISMT).

- Regelmatig rapporteren aan de burgemeester over de status van de cyberbeveiliging en naleving van de NIS2-richtlijn.

4. Information Security Management Team (ISMT)

Rol:

- Tactische en operationele coördinatie van alle aspecten van informatiebeveiliging binnen de gemeente.

Verantwoordelijkheden:

- Uitvoeren van risicoanalyses en kwetsbaarheidsbeoordelingen.

- Ontwikkelen en implementeren van beveiligingsmaatregelen.

- Beheren van incidentrespons en herstelactiviteiten.

- Rapporteren aan de gemeentesecretaris over incidenten, risico's en beveiligingsstatus.

5. IT-afdeling

Rol:

- Implementeren van technische beveiligingsmaatregelen en dagelijkse IT-operaties.

Verantwoordelijkheden:

- Uitvoeren van technische beveiligingsmaatregelen zoals firewalls, antivirus, en encryptie.

- Beheren van toegangscontroles en authenticatiesystemen.

- Uitvoeren van regelmatige back-ups en herstelprocedures.

- Monitoren van netwerken en systemen op verdachte activiteiten.

6. Externe Auditors

Rol:

- Onafhankelijke beoordeling van de naleving van de NIS2-richtlijn en de effectiviteit van de beveiligingsmaatregelen.

Verantwoordelijkheden:

- Uitvoeren van periodieke audits en penetratietests.

- Rapporteren van bevindingen aan de gemeenteraad en gemeentesecretaris.

- Aanbevelen van verbeteringen op basis van auditresultaten.

Governance-structuur Overzicht

```
Gemeenteraad
    |
    | --- Strategisch beleid
    |
Burgemeester
    |
    | --- Handhaving en coördinatie
    |
Gemeentesecretaris (Algemeen Directeur)
    |
    | --- Operationele uitvoering
    |
Information Security Management Team (ISMT)
    |
    | --- Tactische en operationele coördinatie
    |
IT-afdeling
    |
    | --- Technische implementatie
    |
Externe Auditors
    |
```

| --- Onafhankelijke beoordeling

```

## Vragen aan het College van B&W

Strategisch Niveau:

1. Hoe integreert de gemeente de naleving van de NIS2-richtlijn in haar bredere digitale strategie?

2. Welke stappen zijn er genomen om de strategische risico's van cyberaanvallen te verminderen?

Tactisch Niveau:

1. Welke afdelingen en functies zijn verantwoordelijk voor de naleving van de NIS2-richtlijn?

2. Hoe vaak worden risicobeoordelingen en nalevingsaudits uitgevoerd?

Operationeel Niveau:

1. Hoe worden gemeentelijke medewerkers getraind in de vereisten en procedures van de NIS2-richtlijn?

2. Wat zijn de protocollen voor het melden en afhandelen van beveiligingsincidenten?

Door deze governance-structuur en vragen te hanteren, kan de gemeenteraad ervoor zorgen dat de gemeente goed voorbereid is op de naleving van de NIS2-richtlijn en effectief kan reageren op cyberdreigingen.
```

Handboek voor 10 Zorgplichtmaatregelen onder de NIS2-Richtlijn

Dit handboek biedt een gedetailleerd proces voor de implementatie van de tien zorgplichtmaatregelen zoals vereist door de NIS2-richtlijn. Elk Maatregel beschrijft een specifieke maatregel en biedt een stapsgewijze aanpak voor de naleving.

Contents

Samenvatting voor Hoger Management: Handboek voor 10 Zorgplichtmaatregelen

Betekenis van de Zorgplichtmaatregelen

De NIS2-richtlijn vereist dat bedrijven maatregelen nemen om hun netwerk- en informatiesystemen te beschermen tegen incidenten. Dit omvat ook de fysieke omgeving waarin deze systemen zich bevinden. Hieronder wordt een samenvatting gegeven van elk van de tien zorgplichtmaatregelen, samen met een uitleg over hoe u als hoger management deze maatregelen kunt controleren en beoordelen bij uw ondergeschikten.

Maatregel 1: Risicoanalyse en Beveiliging van Informatiesystemen

Betekenis:

Het uitvoeren van een risicoanalyse om bedreigingen en kwetsbaarheden in informatiesystemen te identificeren en te mitigeren.

Controle:

- Vraag om recente rapporten van uitgevoerde risicoanalyses.

- Controleer of er plannen zijn voor periodieke herzieningen van deze analyses.

Maatregel 2: Beveiligingsaspecten op het Gebied van Personeel, Toegangsbeleid en Beheer van Assets

Betekenis:

Het implementeren van strikte beveiligingsmaatregelen voor personeel, toegangscontrole en assetbeheer.

Controle:

- Verifieer of er toegangscontrolesystemen zijn geïmplementeerd en onderhouden.

- Vraag naar het beleid en de procedures voor personeelsbeveiliging en assetbeheer.

Maatregel 3: Bedrijfscontinuïteit, Back-upbeheer en Noodvoorzieningenplannen

Betekenis:

Het opstellen en onderhouden van plannen voor bedrijfscontinuïteit, inclusief back-upbeheer en noodvoorzieningen.

Controle:

- Vraag naar het bedrijfscontinuïteitsplan en de frequentie van back-upprocedures.

- Controleer of er periodieke tests worden uitgevoerd om de effectiviteit van noodvoorzieningen te waarborgen.

Maatregel 4: Incidentenbehandeling

Betekenis:

Het ontwikkelen van procedures voor het effectief afhandelen van beveiligingsincidenten.

Controle:

- Vraag naar het incident response plan en recente incidentrapporten.

- Controleer of er trainingen en oefeningen worden gehouden om de paraatheid van het Incident Response Team te waarborgen.

Maatregel 5: Basis Cyberhygiëne en Trainingen

Betekenis:

Het bevorderen van basis cyberhygiëne en het verzorgen van regelmatige trainingen voor medewerkers op het gebied van cyberbeveiliging.

Controle:

- Vraag naar de opleidingsprogramma's en de frequentie van cyberbeveiligingstrainingen.

- Controleer of er campagnes zijn voor bewustwording en training rondom cyberhygiëne.

Maatregel 6: Beveiliging bij Verwerken, Ontwikkelen en Onderhouden van Netwerk- en Informatiesystemen

Betekenis:

Beveiligingsmaatregelen integreren tijdens het verwerken, ontwikkelen en onderhouden van informatiesystemen.

Controle:

- Vraag naar procedures voor softwareontwikkeling en onderhoud.

- Verifieer of kwetsbaarheden regelmatig worden geanalyseerd en gerapporteerd.

Maatregel 7: Beveiliging van de Toeleverancierssketen

Betekenis:

Het waarborgen van de beveiliging in de gehele toeleveringsketen.

Controle:

- Vraag naar de evaluatieprocedures voor leveranciers en de beveiligingsvereisten die aan hen worden gesteld.

- Controleer of er audits en reviews van leveranciers plaatsvinden.

Maatregel 8: Beleid en Procedures voor Cryptografie en Encryptie

Betekenis:

Het ontwikkelen van beleid en procedures voor het gebruik van cryptografie en encryptie.

Controle:

- Vraag naar het cryptografiebeleid en implementatieprocedures.

- Controleer of de encryptiebeleid voldoet aan de geldende normen en regelgeving.

Maatregel 9: Gebruik van Multifactorauthenticatie en Beveiligde Communicatiesystemen

Betekenis:

Het implementeren van multifactorauthenticatie en het waarborgen van beveiligde communicatiekanalen.

Controle:

- Verifieer of multifactorauthenticatie is geïmplementeerd voor kritieke systemen.

- Vraag naar de beveiligingsmaatregelen voor spraak-, video- en tekstcommunicatie.

Maatregel 10: Beleid en Procedures voor Beoordeling van Cyberbeveiligingsrisico's

Betekenis:

Het ontwikkelen van beleid en procedures om de effectiviteit van beheersmaatregelen te beoordelen.

Controle:

- Vraag naar de methoden en frequentie van risicobeoordelingen.

- Controleer of er processen zijn voor het doorvoeren van verbeteringen op basis van deze beoordelingen.

Conclusie

In Control Blijven

Als hoger management is het cruciaal om de implementatie van deze maatregelen te monitoren en te controleren. Hier zijn enkele manieren om dit effectief te doen:

- Regelmatige Rapportages: Vraag om regelmatige updates en rapporten over de voortgang en naleving van de zorgplichtmaatregelen.

- Stakeholder Engagement: Organiseer bijeenkomsten met afdelingshoofden om de voortgang te bespreken en eventuele knelpunten te identificeren.

- Training en Bewustwording: Zorg ervoor dat alle medewerkers continu worden getraind en zich bewust zijn van hun rol in het nalevingsproces.

- Audits en Beoordelingen: Voer regelmatige interne en externe audits uit om de effectiviteit van de maatregelen te beoordelen en verbeteringen door te voeren.

Door deze maatregelen te implementeren en te controleren, blijft uw organisatie niet alleen compliant met de NIS2-richtlijn, maar versterkt u ook de algehele cyberbeveiliging en weerbaarheid van uw organisatie.

Maatregel 1: Risicoanalyse en Beveiliging van Informatiesystemen

Hier zijn de uitgebreide 10 stappen om een effectief risicoanalyse- en beveiligingsproces voor informatiesystemen te implementeren:

Stap 1: Inventarisatie van Informatie en Systemen

- Actie: Identificeer en documenteer alle kritieke informatie en systemen binnen de organisatie.

- Doel: Begrijpen welke systemen en gegevens essentieel zijn voor de bedrijfsvoering en beveiliging.

Stap 2: Identificatie van Bedreigingen en Kwetsbaarheden

- Actie: Voer een gedetailleerde inventarisatie uit van mogelijke bedreigingen (zoals cyberaanvallen, menselijke fouten, natuurrampen) en kwetsbaarheden in de informatiesystemen.

- Doel: Begrijpen welke bedreigingen en kwetsbaarheden de grootste risico's vormen voor de organisatie.

Stap 3: Risicoanalyse en -beoordeling

- Actie: Gebruik methoden zoals kwalitatieve en kwantitatieve analyses om de geïdentificeerde risico's te beoordelen op basis van hun waarschijnlijkheid en impact.

- Doel: Prioriteer de risico's op basis van hun potentiële impact op de organisatie.

Stap 4: Ontwikkeling van Beveiligingsstrategieën

- Actie: Ontwikkel strategieën en maatregelen om de geïdentificeerde risico's te mitigeren. Dit kan bestaan uit technische oplossingen, beleidsmaatregelen, en organisatorische veranderingen.

- Doel: Verminder de risico's tot een acceptabel niveau.

Stap 5: Implementatie van Beveiligingsmaatregelen

- Actie: Voer de ontwikkelde beveiligingsstrategieën en -maatregelen uit in de organisatie.

- Doel: Zorg ervoor dat de informatie en systemen beschermd zijn tegen de geïdentificeerde bedreigingen.

Stap 6: Monitoring en Detectie

- Actie: Implementeer systemen voor continue monitoring en detectie van bedreigingen en kwetsbaarheden in de informatiesystemen.

- Doel: Identificeer en reageer snel op nieuwe bedreigingen en kwetsbaarheden.

Stap 7: Incidentrespons en Herstel

- Actie: Ontwikkel en implementeer een incidentresponsplan voor het geval er beveiligingsincidenten optreden.

- Doel: Zorg voor een snelle en effectieve respons op incidenten om schade te minimaliseren en snel te herstellen.

Stap 8: Regelmatige Evaluatie en Herziening

- Actie: Voer periodieke evaluaties en herzieningen uit van de risicoanalyse en beveiligingsmaatregelen.

- Doel: Houd de beveiligingsmaatregelen up-to-date en effectief tegen nieuwe bedreigingen.

Stap 9: Training en Bewustwording van Medewerkers

- Actie: Organiseer regelmatige trainingen en bewustwordingssessies voor medewerkers over risicoanalyse en beveiligingsmaatregelen.

- Doel: Verhoog het bewustzijn en de betrokkenheid van medewerkers bij de beveiliging van informatiesystemen.

Stap 10: Documentatie en Rapportage

- Actie: Documenteer alle stappen van de risicoanalyse en beveiligingsmaatregelen en rapporteer regelmatig aan het management.

- Doel: Zorg voor transparantie en verantwoording over de beveiligingsmaatregelen binnen de organisatie.

Conclusie

Door deze gedetailleerde stappen te volgen, kunnen organisaties een robuust proces ontwikkelen voor de risicoanalyse en beveiliging van hun informatiesystemen. Regelmatige evaluaties en updates zorgen ervoor dat de maatregelen effectief blijven en inspelen op nieuwe dreigingen en technologische ontwikkelingen. Dit draagt bij aan de algehele weerbaarheid van de organisatie tegen cyberdreigingen.

Maatregel 2: Beveiligingsaspecten op het Gebied van Personeel, Toegangsbeleid en Beheer van Assets

Hier zijn de uitgebreide 10 stappen om effectieve beveiligingsmaatregelen te implementeren op het gebied van personeel, toegangsbeleid en beheer van assets:

Stap 1: Ontwikkeling van een Beveiligingsbeleid voor Personeel

- Actie: Stel een gedetailleerd beveiligingsbeleid op dat de verantwoordelijkheden en verwachtingen van alle medewerkers beschrijft.

- Doel: Zorg voor een duidelijke richtlijn voor alle medewerkers over hun rol in de beveiliging van de organisatie.

Stap 2: Achtergrondcontroles en Screening van Medewerkers

- Actie: Voer achtergrondcontroles en screening uit voor nieuwe medewerkers, vooral voor diegenen met toegang tot gevoelige informatie.

- Doel: Verifieer de betrouwbaarheid en integriteit van nieuwe medewerkers.

Stap 3: Training en Bewustwording van Medewerkers

- Actie: Ontwikkel en implementeer regelmatige beveiligingstrainingen en bewustwordingssessies voor alle medewerkers.

- Doel: Verhoog het bewustzijn en de kennis van medewerkers over beveiligingsrisico's en best practices.

Stap 4: Ontwikkeling van een Toegangsbeleid

- Actie: Schrijf een formeel toegangsbeleid dat beschrijft wie toegang heeft tot welke systemen en gegevens, gebaseerd op rol en noodzaak.

- Doel: Beperk de toegang tot gevoelige informatie tot geautoriseerde personen.

Stap 5: Implementatie van Toegangscontrolemechanismen

- Actie: Implementeer toegangscontrolemechanismen zoals wachtwoorden, biometrische verificatie, en kaartlezers.

- Doel: Zorg ervoor dat alleen geautoriseerde personen toegang hebben tot kritieke systemen en gegevens.

Stap 6: Regelmatige Evaluatie en Herziening van Toegangsrechten

- Actie: Voer periodieke evaluaties uit van de toegangsrechten van medewerkers en pas deze aan op basis van veranderingen in rol of functie.

- Doel: Houd de toegangsrechten actueel en minimaliseer het risico van ongeautoriseerde toegang.

Stap 7: Beheer van IT-assets

- Actie: Ontwikkel een inventaris van alle IT-assets en implementeer een systeem voor het beheer van deze assets.

- Doel: Houd toezicht op en beheer alle hardware- en software-assets binnen de organisatie.

Stap 8: Beveiliging van Fysieke Assets

- Actie: Implementeer fysieke beveiligingsmaatregelen zoals beveiligde toegangspunten, CCTV, en alarmen om fysieke assets te beschermen.

- Doel: Bescherm fysieke assets tegen diefstal, vandalisme, en onbevoegde toegang.

Stap 9: Beheer van Mobiele en Externe Apparaten

- Actie: Ontwikkel een beleid voor het gebruik en beheer van mobiele en externe apparaten zoals laptops en smartphones.

- Doel: Beveilig mobiele apparaten en zorg voor veilige toegang tot bedrijfsgegevens op afstand.

Stap 10: Documentatie en Rapportage

- Actie: Documenteer alle beveiligingsmaatregelen, toegangscontroles, en assetbeheerprocessen en rapporteer regelmatig aan het management.

- Doel: Zorg voor transparantie en verantwoording over de beveiligingsmaatregelen binnen de organisatie.

Conclusie

Door deze gedetailleerde stappen te volgen, kunnen organisaties een robuust beleid en effectieve maatregelen ontwikkelen voor beveiliging op het gebied van personeel, toegangsbeleid en beheer van assets. Regelmatige evaluaties en updates zorgen ervoor dat de maatregelen effectief blijven en inspelen op nieuwe dreigingen en technologische ontwikkelingen. Dit draagt bij aan de algehele weerbaarheid van de organisatie tegen cyberdreigingen.

Maatregel 3: Bedrijfscontinuïteit, Back-upbeheer en Noodvoorzieningenplannen

Hier zijn de uitgebreide 10 stappen om effectieve maatregelen voor bedrijfscontinuïteit, back-upbeheer en noodvoorzieningen te implementeren:

Stap 1: Ontwikkeling van een Bedrijfscontinuïteitsplan (BCP)

- Actie: Stel een uitgebreid bedrijfscontinuïteitsplan op dat alle kritieke bedrijfsfuncties en processen identificeert en de procedures beschrijft om deze te handhaven tijdens verstoringen.

- Doel: Zorg voor de voortzetting van essentiële bedrijfsactiviteiten in geval van een incident.

Stap 2: Identificatie van Kritieke Systemen en Data

- Actie: Bepaal welke systemen en gegevens cruciaal zijn voor de bedrijfsvoering en documenteer deze in het BCP.

- Doel: Identificeer en prioriteer de belangrijkste systemen en gegevens voor herstel en back-up.

Stap 3: Implementatie van Back-upbeheer

- Actie: Ontwikkel en implementeer een robuust back-upbeheerbeleid dat de frequentie, methoden en opslaglocaties van back-ups beschrijft.

- Doel: Bescherm kritieke gegevens tegen verlies door regelmatige en betrouwbare back-ups.

Stap 4: Ontwikkeling van Noodvoorzieningenplannen

- Actie: Stel noodvoorzieningenplannen op voor verschillende soorten incidenten, zoals natuurrampen, cyberaanvallen en technische storingen.

- Doel: Voorbereiden op diverse noodsituaties en zorgen voor snelle reactie en herstel.

Stap 5: Oefeningen en Tests van het BCP

- Actie: Voer regelmatig oefeningen en tests uit van het bedrijfscontinuïteitsplan om de effectiviteit te beoordelen en medewerkers te trainen.

- Doel: Verbeter de paraatheid van de organisatie en identificeer verbeterpunten.

Stap 6: Implementatie van Alternatieve Communicatiemiddelen

- Actie: Zorg voor alternatieve communicatiemiddelen en -protocollen om de communicatie te waarborgen tijdens een incident.

- Doel: Behoud de communicatie met medewerkers, klanten en stakeholders tijdens verstoringen.

Stap 7: Herstelstrategieën voor IT-systemen

- Actie: Ontwikkel herstelstrategieën voor IT-systemen die snelle herstelprocedures en herstelpunten (RTO en RPO) definiëren.

- Doel: Minimaliseer de downtime en gegevensverlies van kritieke IT-systemen.

Stap 8: Documentatie en Rapportage van Incidenten

- Actie: Documenteer alle incidenten en herstelacties, en voer een grondige analyse uit om lessen te trekken.

- Doel: Verbeter toekomstige respons- en herstelstrategieën op basis van ervaringen.

Stap 9: Regelmatige Herziening en Bijwerking van het BCP

- Actie: Herzie en werk het bedrijfscontinuïteitsplan en de noodvoorzieningenplannen regelmatig bij op basis van veranderende bedrijfsomstandigheden en nieuwe dreigingen.

- Doel: Houd het BCP actueel en relevant voor de organisatie.

Stap 10: Training en Bewustwording van Medewerkers

- Actie: Organiseer regelmatige trainingen en bewustwordingssessies voor medewerkers over hun rollen en verantwoordelijkheden in het BCP.

- Doel: Verhoog het bewustzijn en de kennis van medewerkers over bedrijfscontinuïteit en noodmaatregelen.

Conclusie

Door deze gedetailleerde stappen te volgen, kunnen organisaties een robuust beleid en effectieve maatregelen ontwikkelen voor bedrijfscontinuïteit, back-upbeheer en noodvoorzieningen. Regelmatige evaluaties en updates zorgen ervoor dat de maatregelen effectief blijven en inspelen op nieuwe dreigingen en technologische ontwikkelingen. Dit draagt bij aan de algehele weerbaarheid van de organisatie tegen incidenten en verstoringen.

Maatregel 4: Incidentenbehandeling

Hier zijn de uitgebreide 10 stappen om een effectief incidentenbeheerproces te implementeren:

Stap 1: Identificatie en Klassificatie van Incidenten

- Actie: Ontwikkel een classificatiesysteem voor verschillende soorten incidenten, inclusief criteria voor ernst en impact.

- Doel: Zorg voor een gestructureerde aanpak om incidenten te identificeren en te prioriteren.

Stap 2: Oprichting van een Incident Response Team (IRT)

- Actie: Stel een Incident Response Team samen met duidelijke rollen en verantwoordelijkheden.

- Doel: Zorg voor een gecoördineerde reactie op incidenten met aangewezen teamleden.

Stap 3: Ontwikkeling van een Incident Response Plan (IRP)

- Actie: Schrijf een gedetailleerd incident response plan dat procedures en stappen beschrijft voor het behandelen van incidenten.

- Doel: Voorzie het IRT van een duidelijke gids voor het afhandelen van incidenten.

Stap 4: Implementatie van Detectie- en Monitoringsystemen

- Actie: Implementeer geavanceerde detectie- en monitoringsystemen om incidenten in real-time te detecteren.

- Doel: Verhoog de snelheid en nauwkeurigheid van incidentdetectie.

Stap 5: Training en Oefeningen voor het IRT

- Actie: Voer regelmatige trainingen en simulaties uit om het Incident Response Team voor te bereiden op verschillende scenario's.

- Doel: Zorg ervoor dat het IRT goed voorbereid is op echte incidenten.

Stap 6: Incidentmeldingsprocedures

- Actie: Ontwikkel duidelijke procedures voor het melden van incidenten binnen de organisatie en aan externe partijen, indien nodig.

- Doel: Zorg voor tijdige en accurate rapportage van incidenten.

Stap 7: Incidentanalyse en -beoordeling

- Actie: Voer gedetailleerde analyses uit van elk incident om de oorzaken en gevolgen te begrijpen.

- Doel: Identificeer de worteloorzaken en ontwikkel maatregelen om herhaling te voorkomen.

Stap 8: Herstelmaatregelen en Continuïteit

- Actie: Ontwikkel en implementeer herstelmaatregelen om snel terug te keren naar normale bedrijfsvoering na een incident.

- Doel: Minimaliseer de impact van incidenten op de bedrijfscontinuïteit.

Stap 9: Post-Incident Evaluatie en Lessen

- Actie: Voer een post-incident evaluatie uit om lessen te trekken en verbeterpunten te identificeren.

- Doel: Verbeter de incidentresponsprocessen op basis van ervaringen en evaluaties.

Stap 10: Documentatie en Rapportage

- Actie: Documenteer alle incidenten, inclusief de respons en evaluaties, en rapporteer regelmatig aan het management.

- Doel: Zorg voor transparantie en verantwoording in het incidentbeheerproces.

Conclusie

Door deze gedetailleerde stappen te volgen, kunnen organisaties een robuust incidentenbeheerproces ontwikkelen en implementeren. Regelmatige evaluaties en updates zorgen ervoor dat de maatregelen effectief blijven en inspelen op nieuwe dreigingen en technologische ontwikkelingen. Dit draagt bij aan de algehele weerbaarheid van de organisatie tegen cyberdreigingen.

Maatregel 5: Basis Cyberhygiëne en Trainingen

Hier zijn de uitgebreide 10 stappen om een effectief beleid voor basis cyberhygiëne en trainingen op het gebied van cyberbeveiliging te implementeren:

Stap 1: Ontwikkeling van een Cyberhygiënebeleid

- Actie: Schrijf een gedetailleerd cyberhygiënebeleid dat de basisprincipes en verwachtingen van alle medewerkers beschrijft.

- Doel: Leg een stevige basis voor de veiligheidscultuur binnen de organisatie door duidelijke richtlijnen te bieden.

Stap 2: Identificatie van Cruciale Cyberhygiënepraktijken

- Actie: Bepaal de essentiële cyberhygiënepraktijken die binnen de organisatie moeten worden gevolgd, zoals regelmatig wachtwoordbeheer, software-updates en veilige internetgewoonten.

- Doel: Zorg ervoor dat alle medewerkers de belangrijkste praktijken voor cyberhygiëne begrijpen en volgen.

Stap 3: Ontwikkeling van Trainingsprogramma's

- Actie: Ontwikkel een reeks trainingen die gericht zijn op verschillende aspecten van cyberbeveiliging en cyberhygiëne.

- Doel: Verhoog het bewustzijn en de kennis van medewerkers over cyberveiligheid.

Stap 4: Verplichte Introductietrainingen

- Actie: Voer verplichte introductietrainingen in voor alle nieuwe medewerkers, waarin de basisprincipes van cyberhygiëne en organisatiebeleid worden uitgelegd.

- Doel: Zorg ervoor dat nieuwe medewerkers direct op de hoogte zijn van de beveiligingsvereisten en -verwachtingen.

Stap 5: Regelmatige Opfristrainingen

- Actie: Organiseer periodieke opfristrainingen voor alle medewerkers om hun kennis up-to-date te houden en hen bewust te maken van nieuwe dreigingen en best practices.

- Doel: Voorkom dat de kennis van medewerkers verouderd raakt en verhoog het continu bewustzijn.

Stap 6: Bewustwordingscampagnes

- Actie: Voer regelmatige bewustwordingscampagnes, zoals posters, nieuwsbrieven en e-mails, om de belangrijke aspecten van cyberhygiëne te benadrukken.

- Doel: Houd cyberbeveiliging top-of-mind voor alle medewerkers.

Stap 7: Simulatieoefeningen

- Actie: Voer regelmatig simulatieoefeningen uit, zoals phishing-tests, om de paraatheid van medewerkers te testen en te verbeteren.

- Doel: Identificeer zwakke punten in de kennis en respons van medewerkers en geef gerichte trainingen.

Stap 8: Toegang tot Beveiligingsbronnen

- Actie: Zorg ervoor dat alle medewerkers toegang hebben tot up-to-date beveiligingsbronnen en richtlijnen.

- Doel: Ondersteun medewerkers bij het volgen van best practices door hen de benodigde tools en informatie te bieden.

Stap 9: Evaluatie en Feedback

- Actie: Voer regelmatig evaluaties uit van de effectiviteit van de trainingsprogramma's en bewustwordingsinitiatieven en verzamel feedback van medewerkers.

- Doel: Continu verbeteren van de trainingsprogramma's en bewustwordingscampagnes op basis van feedback en evaluatieresultaten.

Stap 10: Documentatie en Rapportage

- Actie: Documenteer alle trainingen, campagnes en evaluaties en rapporteer regelmatig aan het management over de voortgang en effectiviteit van de cyberhygiëne-initiatieven.

- Doel: Zorg voor volledige transparantie en verantwoording en houd het management op de hoogte van de status van cyberbeveiligingsinitiatieven.

Conclusie

Door deze gedetailleerde stappen te volgen, kunnen organisaties een robuust beleid ontwikkelen en implementeren voor basis cyberhygiëne en trainingen op het gebied van cyberbeveiliging. Regelmatige evaluaties en updates zorgen ervoor dat de maatregelen effectief blijven en inspelen op nieuwe dreigingen en technologische ontwikkelingen. Dit draagt bij aan de algehele weerbaarheid van de organisatie tegen cyberdreigingen.

Maatregel 6: Beveiliging bij het Verwerken, Ontwikkelen en Onderhouden van Netwerk- en Informatiesystemen

Hier zijn de uitgebreide 10 stappen om de beveiliging bij het verwerken, ontwikkelen en onderhouden van netwerk- en informatiesystemen te waarborgen:

Stap 1: Integratie van Beveiliging in de Ontwikkelingslevenscyclus (SDLC)

- Actie: Integreer beveiligingsvereisten in elke fase van de software development life cycle (SDLC), van ontwerp tot implementatie en onderhoud.

- Doel: Zorg ervoor dat beveiliging een fundamenteel onderdeel is van het ontwikkelingsproces.

Stap 2: Beveiligingsvereisten en -specificaties

- Actie: Definieer en documenteer beveiligingsvereisten en -specificaties voor elk project.

- Doel: Bepaal welke beveiligingsmaatregelen noodzakelijk zijn om aan de veiligheidsnormen te voldoen.

Stap 3: Veilige Codering Praktijken

- Actie: Implementeer en bevorder veilige coderingstechnieken en -praktijken binnen het ontwikkelingsteam.

- Doel: Voorkom beveiligingslekken en kwetsbaarheden in de software.

Stap 4: Kwetsbaarheidsbeheer

- Actie: Stel een proces in voor het regelmatig scannen en beheren van kwetsbaarheden in de ontwikkelde software en systemen.

- Doel: Identificeer en verhelp beveiligingsproblemen voordat ze worden uitgebuit.

Stap 5: Regelmatige Beveiligingsreviews en Penetratietests

- Actie: Voer regelmatige beveiligingsreviews en penetratietests uit om zwakke punten te identificeren.

- Doel: Test de robuustheid van de beveiliging en identificeer potentiële kwetsbaarheden.

Stap 6: Patchbeheer en Updates

- Actie: Ontwikkel een patchbeheerbeleid om ervoor te zorgen dat alle systemen up-to-date blijven met de nieuwste beveiligingspatches.

- Doel: Beveilig systemen tegen bekende kwetsbaarheden door tijdig updates en patches toe te passen.

Stap 7: Beheer van Toegang en Rechten

- Actie: Implementeer strikte toegangscontrole en rechtenbeheer om de toegang tot ontwikkelings- en productieomgevingen te beperken.

- Doel: Zorg ervoor dat alleen geautoriseerde gebruikers toegang hebben tot kritieke systemen.

Stap 8: Beveiliging bij Gegevensverwerking en -opslag

- Actie: Implementeer versleuteling en andere beveiligingsmaatregelen voor gegevens in rust en tijdens transmissie.

- Doel: Bescherm gevoelige gegevens tegen ongeautoriseerde toegang en manipulatie.

Stap 9: Incidentrespons en Herstelplanning

- Actie: Ontwikkel een incidentrespons- en herstelplan specifiek voor de ontwikkelings- en onderhoudsprocessen.

- Doel: Zorg voor een snelle en effectieve reactie op beveiligingsincidenten.

Stap 10: Training en Bewustwording voor Ontwikkelaars

- Actie: Bied regelmatige training en bewustwordingsprogramma's aan voor ontwikkelaars over de nieuwste beveiligingspraktijken en -technieken.

- Doel: Verhoog het bewustzijn en de kennis van beveiliging binnen het ontwikkelingsteam.

Conclusie

Door deze gedetailleerde stappen te volgen, kunnen organisaties een robuuste beveiligingsaanpak ontwikkelen voor het verwerken, ontwikkelen en onderhouden van hun netwerk- en informatiesystemen. Regelmatige evaluaties en updates zorgen ervoor dat de beveiligingsmaatregelen actueel blijven en inspelen op nieuwe uitdagingen en technologische ontwikkelingen. Dit draagt bij aan de algehele weerbaarheid van de organisatie tegen cyberdreigingen.

Maatregel 7: Beveiliging van de Toeleverancierskеten

Hier zijn de uitgebreide 10 stappen om de beveiliging van de toeleverancierskеten te waarborgen:

Stap 1: Behoefteanalyse en Inventarisatie van Leveranciers

- Actie: Voer een behoefteanalyse uit om te bepalen welke leveranciers een kritieke rol spelen in uw bedrijfsprocessen.

- Doel: Identificeer alle leveranciers en categoriseer ze op basis van hun impact op de bedrijfsvoering en de kritieke diensten die zij leveren.

Stap 2: Beoordeling van Beveiligingspraktijken van Leveranciers

- Actie: Ontwikkel een vragenlijst of beoordelingscriteria om de beveiligingspraktijken van leveranciers te evalueren.

- Doel: Zorg ervoor dat leveranciers voldoen aan de minimale beveiligingsstandaarden die door uw organisatie zijn vastgesteld.

Stap 3: Contractuele Beveiligingsvereisten

- Actie: Neem specifieke beveiligingsclausules op in contracten met leveranciers die hen verplichten om aan bepaalde beveiligingsstandaarden te voldoen.

- Doel: Bind leveranciers juridisch aan de beveiligingsvereisten van uw organisatie.

Stap 4: Implementatie van Een Toeleverancierskеtenbeheersysteem (Vendor Management System, VMS)

- Actie: Gebruik een VMS om alle leverancierskеteninformatie centraal te beheren en te monitoren.

- Doel: Verbeter het toezicht op en het beheer van de toeleverancierskеten.

Stap 5: Regelmatige Audits en Evaluaties van Leveranciers

- Actie: Voer periodieke audits en evaluaties uit om de naleving van de beveiligingsvereisten door leveranciers te controleren.

- Doel: Identificeer en verhelp zwakke punten in de beveiligingspraktijken van leveranciers.

Stap 6: Continu Risicobeheer

- Actie: Implementeer een continu risicobeheerproces om de risico's van leveranciers regelmatig te beoordelen en te mitigeren.

- Doel: Houd voortdurend toezicht op potentiële risico's binnen de toeleverancierskeketen.

Stap 7: Training en Bewustwording voor Leveranciers

- Actie: Organiseer trainingen en bewustwordingsprogramma's voor leveranciers om hen op de hoogte te brengen van de beveiligingsvereisten en best practices.

- Doel: Zorg ervoor dat leveranciers zich bewust zijn van hun rol in het waarborgen van de beveiliging.

Stap 8: Incidentrespons en Beheersing bij Leveranciers

- Actie: Ontwikkel en implementeer een incidentresponsplan specifiek voor incidenten die verband houden met leveranciers.

- Doel: Zorg voor een snelle en effectieve respons op incidenten in de toeleveringsketen.

Stap 9: Monitoring en Rapportage van Leverancierspresta ties

- Actie: Implementeer systemen voor het continu monitoren van de prestaties van leveranciers en rapporteer regelmatig over hun naleving van beveiligingsvereisten.

- Doel: Houd de prestaties van leveranciers bij en identificeer tijdig eventuele problemen.

Stap 10: Evaluatie en Verbetering van Beveiligingsbeleid voor Leveranciers

- Actie: Voer regelmatige evaluaties uit van het beveiligingsbeleid en de procedures met betrekking tot leveranciers en breng verbeteringen aan op basis van de bevindingen.

- Doel: Continu verbeteren van de beveiligingsmaatregelen om de toeleverancierskеten te beschermen tegen nieuwe dreigingen en risico's.

Conclusie

Door deze gedetailleerde stappen te volgen, kunnen organisaties een robuuste aanpak ontwikkelen voor het beheer en de beveiliging van hun toeleverancierskеten. Regelmatige evaluaties en updates zorgen ervoor dat de maatregelen effectief blijven en aangepast worden aan veranderende dreigingen en technologische ontwikkelingen. Dit draagt bij aan de algehele weerbaarheid van de organisatie tegen cyberdreigingen.

Maatregel 8: Beleid en Procedures over het Gebruik van Cryptografie en Encryptie

Hier zijn de uitgebreide 10 stappen om een uitgebreid cryptografiebeleid en bijbehorende procedures te implementeren:

Stap 1: Behoefteanalyse en Beleidsspecificatie

- Actie: Voer een behoefteanalyse uit om te bepalen welke soorten gegevens en communicatiekanalen cryptografie vereisen.

- Doel: Identificeer kritieke gegevens en systemen die beschermd moeten worden met cryptografische technieken.

Stap 2: Ontwikkeling van een Cryptografiebeleid

- Actie: Schrijf een gedetailleerd cryptografiebeleid dat de gebruiksrichtlijnen voor verschillende soorten gegevens en communicatie beschrijft.

- Doel: Zorg voor een formeel document dat als leidraad dient voor alle cryptografische praktijken binnen de organisatie.

Stap 3: Selectie van Cryptografische Standaarden

- Actie: Kies geschikte cryptografische algoritmen en standaarden, zoals AES, RSA, en SHA-256, in lijn met industriestandaarden en best practices.

- Doel: Garandeer dat de gebruikte cryptografische methoden betrouwbaar en veilig zijn.

Stap 4: Implementatie van Cryptografie in Systemen

- Actie: Integreer cryptografische technieken in alle relevante systemen en applicaties, inclusief gegevens in rust en tijdens transmissie.

- Doel: Bescherm gegevens tegen ongeautoriseerde toegang en manipulatie.

Stap 5: Beheer van Cryptografische Sleutels

- Actie: Ontwikkel procedures voor het genereren, distribueren, opslaan, en intrekken van cryptografische sleutels.

- Doel: Zorg voor een veilig beheer van sleutels om de integriteit van de cryptografische processen te waarborgen.

Stap 6: Training en Bewustwording

- Actie: Train alle relevante medewerkers in het cryptografiebeleid en de procedures voor sleutelbeheer.

- Doel: Verhoog het bewustzijn en de kennis van cryptografische technieken binnen de organisatie.

Stap 7: Monitoring en Audit van Cryptografisch Gebruik

- Actie: Implementeer monitoringtools om het gebruik van cryptografie in systemen te bewaken en regelmatige audits uit te voeren.

- Doel: Zorg voor naleving en detecteer eventuele misconfiguraties of misbruik van cryptografische technieken.

Stap 8: Incidentrespons voor Cryptografiegerelateerde Incidenten

- Actie: Ontwikkel specifieke procedures voor het omgaan met incidenten waarbij cryptografie is betrokken, zoals sleutelcompromittering.

- Doel: Zorg voor een snelle en effectieve respons om de impact van dergelijke incidenten te minimaliseren.

Stap 9: Regelmatige Evaluatie en Bijwerking

- Actie: Voer periodieke evaluaties uit van het cryptografiebeleid en de procedures, en werk deze bij op basis van nieuwe dreigingen en technologische ontwikkelingen.

- Doel: Houd het beleid en de procedures actueel en effectief.

Stap 10: Documentatie en Rapportage

- Actie: Documenteer alle aspecten van het cryptografiebeleid, inclusief beleidswijzigingen, trainingssessies, audits en incidenten.

- Doel: Zorg voor volledige transparantie en verantwoording over de cryptografische praktijken binnen de organisatie.

Conclusie

Door deze gedetailleerde stappen te volgen, kunnen organisaties een robuust cryptografiebeleid ontwikkelen en implementeren, waarmee zij gevoelige gegevens en communicatie effectief kunnen beschermen tegen cyberdreigingen. Regelmatige evaluaties en updates zorgen ervoor dat de maatregelen actueel blijven en inspelen op nieuwe uitdagingen en technologieën.

Maatregel 9: Het Gebruik van Multifactor Authenticatie, Beveiligde Spraak-, Video- en Tekstcommunicatie en Beveiligde Noodcommunicatiesystemen

Stap 1: Behoefteanalyse en Planning

- Actie: Voer een behoefteanalyse uit om te bepalen welke systemen en gegevens multifactor authenticatie (MFA) en beveiligde communicatiesystemen vereisen.

- Doel: Identificeer kritieke systemen en communicatiekanalen die extra beveiligingslagen nodig hebben.

Stap 2: Selectie van Multifactor Authenticatie (MFA) Oplossingen

- Actie: Onderzoek en selecteer geschikte MFA-oplossingen die passen bij de beveiligingsvereisten van uw organisatie.

- Doel: Zorg voor een robuuste MFA-oplossing die effectief is tegen ongeautoriseerde toegang.

Stap 3: Implementatie van MFA

- Actie: Implementeer MFA op alle kritieke systemen en zorg voor integratie met bestaande beveiligingsinfrastructuren.

- Doel: Verhoog de beveiliging door een extra authenticatielaag toe te voegen.

Stap 4: Beveiligde Spraak-, Video- en Tekstcommunicatie

- Actie: Selecteer en implementeer oplossingen voor beveiligde spraak-, video- en tekstcommunicatie.

- Doel: Zorg ervoor dat alle communicatiekanalen versleuteld zijn om interceptie en afluisteren te voorkomen.

Stap 5: Beveiligde Noodcommunicatiesystemen

- Actie: Ontwikkel en implementeer beveiligde noodcommunicatiesystemen die kunnen worden gebruikt in geval van noodsituaties.

- Doel: Waarborg communicatie tijdens incidenten en noodsituaties.

Stap 6: Training en Bewustwording

- Actie: Train alle medewerkers in het gebruik van MFA en beveiligde communicatiesystemen.

- Doel: Verhoog het bewustzijn en de kennis over beveiligde communicatiepraktijken.

Stap 7: Monitoring en Onderhoud

- Actie: Implementeer monitoringtools om de effectiviteit van MFA en beveiligde communicatiesystemen te bewaken en voer regelmatig onderhoud uit.

- Doel: Zorg ervoor dat de systemen up-to-date en effectief blijven.

Stap 8: Incidentrespons en Herstel

- Actie: Ontwikkel procedures voor het reageren op incidenten waarbij beveiligde communicatiekanalen betrokken zijn.

- Doel: Zorg voor een snelle en effectieve respons op beveiligingsincidenten.

Stap 9: Evaluatie en Verbetering

- Actie: Voer regelmatige evaluaties uit van de effectiviteit van MFA en beveiligde communicatiesystemen en breng verbeteringen aan waar nodig.

- Doel: Continu verbeteren van de beveiligingsmaatregelen.

Stap 10: Documentatie en Rapportage

- Actie: Documenteer alle stappen, procedures en evaluatieresultaten met betrekking tot MFA en beveiligde communicatiesystemen.

- Doel: Zorg voor volledige transparantie en verantwoording.

Maatregel 10: Beleid en Procedures om de Effectiviteit van Beheersmaatregelen van Cyberbeveiligingsrisico's te Beoordelen

Stap 1: Ontwikkeling van Beoordelingsbeleid

- Actie: Stel een formeel beleid op voor de beoordeling van de effectiviteit van beheersmaatregelen voor cyberbeveiligingsrisico's.

- Doel: Zorg voor een gestructureerde aanpak voor risicobeoordelingen.

Stap 2: Vaststellen van Beoordelingscriteria

- Actie: Definieer duidelijke criteria en meetbare indicatoren voor het beoordelen van beheersmaatregelen.

- Doel: Objectieve en consistente beoordeling van risicobeheersing.

Stap 3: Periodieke Risicobeoordelingen

- Actie: Voer periodieke risicobeoordelingen uit volgens een vast schema.

- Doel: Regelmatig inzicht krijgen in de effectiviteit van de beheersmaatregelen.

Stap 4: Gebruik van Beoordelingstools

- Actie: Implementeer tools en technieken voor het beoordelen van cyberbeveiligingsrisico's.

- Doel: Verbeter de nauwkeurigheid en efficiëntie van risicobeoordelingen.

Stap 5: Analyse van Beoordelingsresultaten

- Actie: Analyseer de resultaten van de risicobeoordelingen om trends en zwakke punten te identificeren.

- Doel: Inzicht krijgen in gebieden die verbetering behoeven.

Stap 6: Implementatie van Verbeteringen

- Actie: Ontwikkel en implementeer verbeteringsplannen op basis van de resultaten van risicobeoordelingen.

- Doel: Versterken van de cyberbeveiligingsmaatregelen.

Stap 7: Documentatie en Rapportage

- Actie: Documenteer alle risicobeoordelingen, analyses en verbetermaatregelen.

- Doel: Zorg voor volledige transparantie en verantwoording.

Stap 8: Training en Bewustwording

- Actie: Train medewerkers over het beleid en de procedures voor risicobeoordeling en de implementatie van verbeteringen.

- Doel: Verhoog het bewustzijn en de betrokkenheid bij risicobeheer.

Stap 9: Externe Beoordelingen en Audits

- Actie: Laat periodiek externe beoordelingen en audits uitvoeren om de effectiviteit van de risicobeoordelingen en beheersmaatregelen te valideren.

- Doel: Zorg voor een objectieve en onpartijdige evaluatie.

Stap 10: Continue Verbetering

- Actie: Pas een continu verbeteringsproces toe waarbij feedback van risicobeoordelingen en audits wordt gebruikt om de beheersmaatregelen voortdurend te verbeteren.

- Doel: Houd de cyberbeveiligingsmaatregelen up-to-date en effectief tegen nieuwe dreigingen.

Conclusie

Dit handboek biedt een gestructureerde aanpak voor de implementatie van de tien zorgplichtmaatregelen zoals vereist door de NIS2-richtlijn. Door deze stappen zorgvuldig te volgen, kunnen organisaties hun netwerk- en informatiesystemen effectief beschermen tegen incidenten en voldoen aan de wettelijke eisen. Het is essentieel om regelmatig evaluaties en verbeteringen door te voeren om de beveiligingsmaatregelen effectief te houden en aan te passen aan veranderende dreigingen en technologieën.

Handboek voor Cyberbeveiligingswet NIS2-Richtlijn, Registratieplicht, Meldplicht en Toezicht

Dit handboek moet dienen als een levende documentatie die regelmatig wordt bijgewerkt om te blijven voldoen aan de nieuwste regelgeving en best practices van de NIS2-Richtlijn.

Hier focussen we op de ongeschreven regels van de Registratieplicht, Meldplicht en Toezicht die de NIS2-Richtlijn voorschrijft.

Contents

Samenvatting voor Hoger Management: Cyberbeveiligingswet en NIS2

Betekenis van de Cyberbeveiligingswet en NIS2

De Europese Cyberbeveiligingswet en de NIS2-richtlijn stellen strenge eisen aan de beveiliging van netwerk- en informatiesystemen van essentiële diensten en belangrijke infrastructuren. Dit betekent dat uw organisatie verplicht is om zich te registreren bij het Nationaal Cyber Security Centrum (NCSC), meldingen te doen van significante cyberincidenten, en onder toezicht komt te staan van aangewezen toezichthouders.

Hoofdtaken en Acties

1. Registratieplicht

- Registratie bij NCSC: Uw organisatie moet alle relevante gegevens bijwerken en zich registreren bij het NCSC.

- Data Governance en IT-beheer: Het implementeren van strikte data governance praktijken en IT-beheerprocessen om te voldoen aan de wetgeving.

- Periodieke Herziening: Jaarlijkse herzieningen en regelmatige audits om de nauwkeurigheid van de registratiegegevens te waarborgen.

2. Meldplicht

- Incidentdetectie en -respons: Gebruik van geavanceerde monitoring tools en een gestandaardiseerd incidentresponsprotocol om cyberincidenten effectief te beheren en te melden.

- Post-Incident Analyse: Uitvoeren van gedetailleerde analyses na incidenten om toekomstige voorvallen te voorkomen en processen te verbeteren.

3. Toezicht

- Onafhankelijke Audits: Periodieke audits door externe partijen om de naleving van de wet te controleren.

- Correctieve Acties en Continu Verbeteren: Implementeren van correctieve acties op basis van auditbevindingen en doorlopende evaluaties om de nalevingsprocessen te verbeteren.

Hoe te Vragen aan Ondersteunende Teams

Als hoger management is het essentieel om de volgende vragen aan uw teams te stellen om ervoor te zorgen dat u in control blijft:

1. Registratie

- Is onze organisatie volledig geregistreerd bij het NCSC en zijn de gegevens up-to-date?

- Hoe vaak worden de registratiegegevens herzien en bijgewerkt?

2. Incidentbeheer

- Welke systemen hebben we geïmplementeerd voor het detecteren en melden van cyberincidenten?

- Hoe effectief is ons incidentresponsprotocol en hoe wordt het personeel hierin getraind?

3. Naleving en Toezicht

- Wanneer was onze laatste onafhankelijke audit en wat waren de bevindingen?

- Welke correctieve acties zijn geïmplementeerd op basis van auditresultaten en hoe worden deze acties gemonitord?

In Control Blijven

Om in control te blijven over de naleving van de Cyberbeveiligingswet en de NIS2-richtlijn:

- Regelmatige Rapportages: Zorg ervoor dat u regelmatig updates en rapportages ontvangt over de status van registratie, incidentbeheer, en naleving.

- Stakeholder Engagement: Organiseer regelmatig bijeenkomsten met alle relevante stakeholders om de voortgang te bespreken en feedback te ontvangen.

- Training en Bewustwording: Investeer in continue training en bewustwordingsprogramma's voor alle medewerkers om ervoor te zorgen dat iedereen op de hoogte is van hun rol en verantwoordelijkheid in het nalevingsproces.

Door deze maatregelen te nemen, kunt u als hoger management effectief toezicht houden op de naleving van de Cyberbeveiligingswet en de NIS2-richtlijn binnen uw organisatie en bijdragen aan een sterke en veerkrachtige cyberbeveiligingspositie.

Hoofdstuk 1: Inleiding

- Doel van het Handboek: Het doel van dit handboek is om organisaties te helpen voldoen aan de eisen van de Cyberbeveiligingswet, inclusief registratieplicht, meldplicht, en toezicht.

- Scope: Dit handboek is van toepassing op alle organisaties die onder de Cyberbeveiligingswet vallen, zoals gedefinieerd door het Nationaal Cyber Security Centrum (NCSC).

Hoofdstuk 2: Registratieplicht

1: Identificatie van de Organisatie

- Doel: Bepaal of uw organisatie valt onder de Cyberbeveiligingswet.

- Actie: Controleer de lijst met essentiële diensten en sectoren die vallen onder de wet.

2: Voorbereiding van de Registratie

- Doel: Verzamel alle benodigde informatie voor de registratie.

- Actie: Verzamel de volgende gegevens:

  - Naam van de organisatie

  - Contactgegevens

  - Sector en type essentiële dienst

  - Informatie over de IT- en beveiligingsinfrastructuur

3: Registratie bij het NCSC

- Doel: Registreer uw organisatie officieel bij het NCSC.

- Actie:

  - Ga naar de website van het NCSC en zoek naar het registratieformulier.

  - Vul het formulier in met de verzamelde informatie.

  - Dien het formulier in en ontvang een bevestiging van registratie.

4: Communicatie en Bewustwording

- Doel: Verhoog de interne bewustwording over de registratieplicht.

- Actie:

  - Informeer alle relevante afdelingen over de registratievereisten en hun verantwoordelijkheden.

  - Organiseer workshops en trainingssessies om het belang van registratie en naleving te benadrukken.

5: Documentatie en Dossiervorming

- Doel: Zorg voor volledige en nauwkeurige documentatie van de registratieprocedure.

- Actie:

  - Houd een register bij van alle ingediende en goedgekeurde registraties.

  - Bewaar kopieën van alle communicatie met het NCSC en andere relevante instanties.

6: Periodieke Herziening

- Doel: Zorg voor een jaarlijkse herziening van de registratie-informatie.

- Actie:

  - Stel een team aan om jaarlijks de registratiegegevens te herzien en bij te werken.

  - Dien eventuele wijzigingen in bij het NCSC en zorg voor bevestiging van deze updates.

7: Evaluatie van Beveiligingsmaatregelen

- Doel: Evalueer de huidige beveiligingsmaatregelen om te voldoen aan de registratievereisten.

- Actie:

  - Voer een uitgebreide beoordeling uit van de bestaande beveiligingsmaatregelen.

  - Documenteer de resultaten en identificeer gebieden die moeten worden verbeterd.

8: Beveiligingscertificering

- Doel: Zorg voor relevante beveiligingscertificeringen als onderdeel van de registratie.

- Actie:

  - Behaal certificeringen zoals ISO 27001 om de beveiligingsstandaarden van de organisatie te bevestigen.

  - Bewaar certificeringen als bewijs van naleving tijdens de registratie.

9: Integratie met HR-systemen

- Doel: Zorg ervoor dat de registratie-informatie regelmatig wordt bijgewerkt via HR-systemen.

- Actie:

  - Koppel HR-systemen aan het registratieproces om veranderingen in personeel automatisch te verwerken.

  - Implementeer een controlemechanisme om de nauwkeurigheid van de gegevens te waarborgen.

10: Implementatie van Beveiligingsnormen

- Doel: Zorg ervoor dat de organisatie voldoet aan erkende beveiligingsnormen.

- Actie:

  - Implementeer beveiligingsnormen zoals ISO/IEC 27001 en NIST Cybersecurity Framework.

  - Documenteer de naleving van deze normen als onderdeel van de registratie.

11: Interne Beoordelingen

- Doel: Voer interne beoordelingen uit om naleving te garanderen.

- Actie:

  - Plan en voer interne beoordelingen uit om te verifiëren dat de registratie-informatie accuraat en up-to-date is.

  - Maak rapporten van de bevindingen en corrigeer eventuele tekortkomingen.

12: Communicatie met Stakeholders

- Doel: Communiceer de registratievereisten en -status naar alle relevante stakeholders.

- Actie:

  - Stel een communicatieplan op om alle interne en externe stakeholders te informeren over de registratievereisten en -status.

  - Houd regelmatige updates en briefings om iedereen op de hoogte te houden van de voortgang en eventuele wijzigingen.

13: Ondersteuning van Management en Raad van Bestuur

- Doel: Betrek het management en de raad van bestuur actief bij het registratieproces.

- Actie:

  - Organiseer informatiesessies voor het management om hen te informeren over hun verantwoordelijkheden onder de Cyberbeveiligingswet.

  - Stel rapportages op voor de raad van bestuur om hen op de hoogte te houden van de voortgang van de registratie en naleving.

14: Escalatieprocedures voor Registratieproblemen

- Doel: Ontwikkel een duidelijke escalatieprocedure voor problemen die optreden tijdens het registratieproces.

- Actie:

  - Definieer een escalatiepad en verantwoordelijkheden voor het oplossen van registratieproblemen.

  - Documenteer en communiceer deze procedures naar alle relevante betrokkenen.

15: Evaluatie van Externe Partners en Leveranciers

- Doel: Zorg dat externe partners en leveranciers ook voldoen aan de registratievereisten.

- Actie:

  - Voer beoordelingen uit van de beveiligingspraktijken van externe partners en leveranciers.

  - Zorg dat contracten clausules bevatten die naleving van de Cyberbeveiligingswet vereisen.

16: Implementatie van IT-beheerprocessen

- Doel: Zorg voor een gestroomlijnde aanpak van IT-beheerprocessen om de naleving van de Cyberbeveiligingswet te waarborgen.

- Actie:

  - Implementeer ITIL-processen voor incidentbeheer, probleembeheer, en wijzigingsbeheer.

  - Documenteer alle processen en zorg voor regelmatige updates en herzieningen.

17: Monitoring en Evaluatie van Registratiegegevens

- Doel: Continu monitoren en evalueren van registratiegegevens om nauwkeurigheid en volledigheid te waarborgen.

- Actie:

  - Gebruik monitoringtools om gegevens continu te evalueren en afwijkingen te identificeren.

  - Stel een evaluatieteam aan dat verantwoordelijk is voor het regelmatig controleren en bijwerken van registratiegegevens.

18: Beoordeling van Juridische Aspecten

- Doel: Zorg ervoor dat alle juridische aspecten van de registratie worden nageleefd.

- Actie:

 - Raadpleeg juridische adviseurs om ervoor te zorgen dat de registratieprocessen voldoen aan alle wettelijke vereisten.

 - Documenteer alle juridische beoordelingen en bewaar deze voor toekomstige referentie.

19: Onderzoek naar Best Practices

- Doel: Blijf op de hoogte van best practices in de industrie.

- Actie:

 - Doe regelmatig onderzoek naar de nieuwste best practices voor cyberbeveiliging.

 - Pas deze best practices toe in de registratieprocedures en -processen.

20: Betrekken van Externe Adviseurs

- Doel: Zorg voor externe expertise bij de registratie en naleving.

- Actie:

 - Huur externe adviseurs in om uw registratieprocessen te beoordelen en advies te geven.

 - Gebruik de inzichten van deze adviseurs om processen te verbeteren en naleving te waarborgen.

21: Evaluatie van Risicomanagementstrategieën

- Doel: Optimaliseer risicomanagementstrategieën voor betere naleving.

- Actie:

 - Beoordeel de bestaande risicomanagementstrategieën en hun effectiviteit.

 - Integreer bevindingen in de registratie- en nalevingsprocessen om risico's beter te beheren.

22: Implementatie van Data Governance

- Doel: Verbetering van de governance en het beheer van gegevens binnen de organisatie.

- Actie:

  - Stel een data governance beleid op dat de verantwoordelijken voor data-eigendom en databeheer identificeert.

  - Zorg ervoor dat gegevens nauwkeurig, up-to-date en beveiligd zijn volgens de richtlijnen van de Cyberbeveiligingswet.

23: Onderhoud en Actualisatie van Registratiegegevens

- Doel: Continue actualisatie van registratiegegevens om nauwkeurigheid en volledigheid te waarborgen.

- Actie:

  - Voer halfjaarlijkse audits uit om de actualiteit van registratiegegevens te controleren.

  - Update registratiegegevens onmiddellijk bij organisatorische wijzigingen zoals nieuwe technologieën of wijzigingen in contactinformatie.

24: Training van Registratiebeheerders

- Doel: Verzekeren dat medewerkers die verantwoordelijk zijn voor registratie goed opgeleid zijn.

- Actie:

  - Ontwikkel een trainingsprogramma voor registratiebeheerders, inclusief richtlijnen voor registratie, data-invoer en gegevensbeheer.

  - Voer jaarlijkse opfriscursussen uit om ervoor te zorgen dat beheerders op de hoogte blijven van wijzigingen in de regelgeving.

25: Evaluatie van Organisatorische Structuur

- Doel: Zorg ervoor dat de organisatorische structuur de naleving van de Cyberbeveiligingswet ondersteunt.

- Actie:

  - Beoordeel of de huidige organisatorische structuur voldoende middelen en ondersteuning biedt voor naleving.

  - Voer wijzigingen door indien nodig om te zorgen dat er duidelijke rollen en verantwoordelijkheden zijn voor nalevingsactiviteiten.

26: Opstellen van Registratiebeleid

- Doel: Formuleer een formeel beleid voor de registratieprocessen.

- Actie:

  - Schrijf een gedetailleerd registratiebeleid dat alle stappen, vereisten en verantwoordelijkheden beschrijft.

  - Zorg dat het beleid wordt goedgekeurd door het management en regelmatig wordt herzien en bijgewerkt.

27: Beheer van Gebruikersrechten en Toegang

- Doel: Beveilig de registratiegegevens door middel van strikt beheer van gebruikersrechten en toegang.

- Actie:

  - Stel toegangscontrolemechanismen in om te zorgen dat alleen geautoriseerde personen toegang hebben tot registratiegegevens.

  - Gebruik rollen-gebaseerde toegangscontrole (RBAC) om toegang te beheren op basis van functie en verantwoordelijkheden.

28: Evaluatie van IT-infrastructuur

- Doel: Zorg ervoor dat de IT-infrastructuur in lijn is met de eisen van de Cyberbeveiligingswet.

- Actie:

  - Voer een grondige evaluatie uit van de huidige IT-infrastructuur.

  - Identificeer gebieden die verbetering behoeven om aan de wetgeving te voldoen.

29: Periodieke Herziening en Bijwerking

- Doel: Regelmatige herziening en bijwerking van de registratie-informatie.

- Actie:

  - Plan jaarlijkse herzieningen van alle registratie-informatie om nauwkeurigheid te waarborgen.

  - Update de informatie zodra er veranderingen plaatsvinden in de organisatie, zoals wijzigingen in management of IT-systemen.

30: Opleiding en Bewustzijn

- Doel: Zorg ervoor dat alle medewerkers zich bewust zijn van hun rol in het registratieproces.

- Actie:

  - Ontwikkel en implementeer een uitgebreid trainingsprogramma over de registratieplicht en de Cyberbeveiligingswet.

  - Houd regelmatig opfriscursussen om medewerkers up-to-date te houden.

Hoofdstuk 3: Meldplicht

1: Incidentidentificatie

- Doel: Bepaal of een incident meldingswaardig is.

- Actie: Beoordeel incidenten op basis van:

  - Aantal personen dat door de verstoring is geraakt

  - Tijdsduur van de verstoring

  - Mogelijke financiële verliezen

2: Melden aan de Toezichthouder

- Doel: Meld incidenten die de verlening van de essentiële dienst aanzienlijk verstoren.

- Actie:

  - Neem contact op met de aangewezen toezichthouder voor uw sector.

  - Voorzie hen van een gedetailleerd incidentrapport dat de aard en impact van de verstoring beschrijft.

3: Melden aan het CSIRT

- Doel: Meld cyberincidenten bij het Computer Security Incident Response Team.

- Actie:

  - Contacteer het CSIRT via de door hen verstrekte kanalen.

  - Voorzie hen van een gedetailleerd incidentrapport, inclusief technische details en genomen tegenmaatregelen.

  - Volg de instructies van het CSIRT voor verdere actie en assistentie.

4: Incident Response Team (IRT)

- Doel: Vorm een gespecialiseerd team dat verantwoordelijk is voor het beheren van incidentmeldingen.

- Actie:

  - Stel een Incident Response Team (IRT) samen met leden uit IT, juridische zaken, en communicatie.

  - Ontwikkel en implementeer een incident response plan dat duidelijke rollen en verantwoordelijkheden bevat.

5: Training en Simulaties

- Doel: Voorbereiden op mogelijke incidenten door middel van training en simulaties.

- Actie:

  - Voer regelmatig trainingen en simulaties uit om het IRT en andere relevante medewerkers voor te bereiden op incidentmeldingen.

  - Documenteer leerpunten uit deze oefeningen en pas het incident response plan indien nodig aan.

6: Integratie met Andere Systemen

- Doel: Zorg voor een naadloze integratie van het meldingssysteem met andere bedrijfsprocessen.

- Actie:

  - Integreer het meldingssysteem met de bestaande IT- en communicatiesystemen om snelle en efficiënte meldingen te garanderen.

  - Zorg voor een duidelijke en snelle rapportagelijn naar het management.

7: Implementatie van Incidentdetectiesystemen

- Doel: Zorg voor geavanceerde systemen voor het detecteren van incidenten.

- Actie:

  - Implementeer SIEM (Security Information and Event Management) systemen om realtime incidenten te detecteren en te melden.

  - Train medewerkers in het gebruik van deze systemen.

8: Incident Classificatie en Prioritering

- Doel: Classificeer en prioriteer incidenten op basis van hun impact.

- Actie:

  - Ontwikkel een classificatiesysteem voor incidenten (bijv. laag, middel, hoog).

  - Prioriteer incidenten op basis van hun potentiële impact op de organisatie en meld deze dienovereenkomstig.

9: Opleidingsprogramma voor Incidentrespons

- Doel: Voorzie medewerkers van de nodige training om effectief op incidenten te reageren.

- Actie:

  - Ontwikkel en implementeer een opleidingsprogramma gericht op incidentrespons.

  - Houd regelmatig trainingssessies en simulaties om het bewustzijn en de vaardigheden te verbeteren.

10: Integratie van Incidentmanagement Systemen

- Doel: Zorg voor een geïntegreerde aanpak van incidentbeheer.

- Actie:

  - Implementeer een Incident Management System (IMS) dat naadloos integreert met bestaande IT- en communicatiesystemen.

  - Zorg voor automatische meldingen en alerts om incidenten snel te kunnen identificeren en rapporteren.

11: Samenwerking met Externe Partijen

- Doel: Werk samen met externe partijen om incidenten effectief te beheren.

- Actie:

- Stel samenwerkingsafspraken op met externe cybersecurity-dienstverleners en incident response teams.

- Organiseer gezamenlijke oefeningen en simulaties om de samenwerking te testen en te verbeteren.

12: Evaluatie en Verbetering van Meldprocessen

- Doel: Continu verbeteren van de meldprocessen.

- Actie:

- Voer na elk incident een evaluatie uit om de effectiviteit van het meldproces te beoordelen.

- Documenteer verbeterpunten en implementeer deze in toekomstige meldprocessen.

13: Incident Rapportage en Documentatie

- Doel: Zorg voor gedetailleerde documentatie van alle gemelde incidenten.

- Actie:

- Ontwikkel een standaard sjabloon voor incidentrapportages.

- Zorg dat elke melding een gedetailleerd verslag bevat van de aard van het incident, de impact, de genomen maatregelen en de uiteindelijke oplossing.

14: Communicatie met Getroffenen

- Doel: Informeer alle betrokkenen over incidenten en de genomen maatregelen.

- Actie:

- Stel een communicatieprotocol op om betrokkenen op de hoogte te stellen van incidenten die hen aangaan.

- Biedt transparante updates over de voortgang en oplossingsmaatregelen.

15: Beoordeling van de Effectiviteit van Incidentrespons

- Doel: Evalueer de effectiviteit van de respons op incidenten om verbeteringen door te voeren.

- Actie:

  - Voer na elk incident een evaluatie uit met het Incident Response Team.

  - Identificeer en documenteer verbeterpunten en implementeer deze in het incident response plan.

16: Coördinatie met Wetshandhavingsinstanties

- Doel: Samenwerken met wetshandhavingsinstanties bij ernstige incidenten.

- Actie:

  - Stel protocollen op voor samenwerking met politie en andere wetshandhavingsinstanties.

  - Implementeer een communicatieplan om snel informatie te delen met deze instanties tijdens incidenten.

17: Crisiscommunicatieplan

- Doel: Ontwikkel een crisiscommunicatieplan om effectief te communiceren tijdens ernstige incidenten.

- Actie:

  - Ontwikkel een gedetailleerd crisiscommunicatieplan dat stappen bevat voor interne en externe communicatie tijdens een incident.

  - Train communicatiepersoneel in het uitvoeren van het crisiscommunicatieplan.

18: Rapportage aan Aandeelhouders en Publiek

- Doel: Zorg voor transparantie en verantwoording naar aandeelhouders en het publiek.

- Actie:

 - Ontwikkel een rapportagestrategie om incidenten en de genomen maatregelen te communiceren naar aandeelhouders en het publiek.

 - Publiceer regelmatig updates en rapporten over de naleving van de meldplicht en incidentrespons.

19: Integratie van Threat Intelligence

- Doel: Gebruik threat intelligence om incidenten beter te begrijpen en te beheren.

- Actie:

 - Integreer threat intelligence feeds in uw meld- en incidentbeheersystemen.

 - Analyseer deze intelligence om proactief potentiële bedreigingen te identificeren en aan te pakken.

20: Automatisering van Incidentmeldingen

- Doel: Verbeter de efficiëntie van incidentmeldingen door automatisering.

- Actie:

 - Gebruik geautomatiseerde systemen om incidenten snel te detecteren en te melden.

 - Zorg voor automatische rapportagesystemen die de nodige informatie direct naar de toezichthouder sturen.

21: Herstel na Incidenten

- Doel: Zorg voor effectieve herstelplannen na een incident.

- Actie:

 - Ontwikkel en implementeer gedetailleerde herstelplannen voor verschillende soorten incidenten.

 - Voer regelmatig hersteltrainingen uit om de effectiviteit van deze plannen te testen.

22: Gebruik van Incident Response Playbooks

- Doel: Standaardiseren van reacties op incidenten met behulp van gedocumenteerde procedures.

- Actie:

  - Ontwikkel incident response playbooks voor verschillende soorten incidenten (bijv. datalekken, ransomware-aanvallen).

  - Train het Incident Response Team (IRT) in het gebruik van deze playbooks tijdens incidenten.

23: Uitwisseling van Informatie met Industriepartners

- Doel: Verbetering van de incidentrespons door samenwerking met industriepartners.

- Actie:

  - Stel procedures op voor het delen van informatie over incidenten met andere organisaties in dezelfde sector.

  - Neem deel aan cybersecurity-initiatieven en -fora om de uitwisseling van informatie te bevorderen.

24: Regelmatige Evaluatie van Incidentmeldingen

- Doel: Continue verbetering van de meldprocedures door evaluatie en feedback.

- Actie:

  - Voer na elk gemeld incident een evaluatie uit om de effectiviteit van de meldprocedures te beoordelen.

  - Documenteer lessen en verbeteringen en integreer deze in toekomstige procedures.

25: Implementatie van Cyber Insurance

- Doel: Verminder de financiële impact van cyberincidenten door verzekering.

- Actie:

 - Onderzoek en sluit een cyberverzekering af die dekking biedt voor incidenten die onder de meldplicht vallen.

 - Werk samen met de verzekeringsmaatschappij om te begrijpen welke incidenten gedekt zijn en hoe meldingsprocedures moeten worden gevolgd.

26: Ontwikkeling van Incidentclassificatiesysteem

- Doel: Classificeer incidenten om prioriteit en aanpak te bepalen.

- Actie:

 - Ontwikkel een systeem voor het classificeren van incidenten op basis van ernst, impact en type.

 - Train het Incident Response Team in het gebruik van dit classificatiesysteem om snel en adequaat te reageren.

27: Periodieke Incident Drills

- Doel: Bereid de organisatie voor op echte incidenten door middel van oefeningen.

- Actie:

 - Organiseer regelmatig incident drills en simulaties om de paraatheid en respons van het Incident Response Team te testen.

 - Documenteer en evalueer de resultaten van deze drills om verbeterpunten te identificeren en door te voeren.

28: Implementatie van Monitoring Tools

- Doel: Verbeter de incidentdetectie en -respons door monitoring tools te implementeren.

- Actie:

  - Installeer en configureer geavanceerde monitoring tools om cyberincidenten in real-time te detecteren.

  - Zorg voor een centrale monitoringlocatie waar alle gegevens worden verzameld en geanalyseerd.

29: Incidentrespons Protocol

- Doel: Ontwikkel een gestandaardiseerd incidentresponsprotocol.

- Actie:

  - Stel duidelijke richtlijnen op voor het reageren op verschillende soorten cyberincidenten.

  - Train alle relevante medewerkers in het gebruik van het incidentresponsprotocol.

30: Post-Incident Analyse

- Doel: Voer gedetailleerde analyses uit na incidenten om toekomstige voorvallen te voorkomen.

- Actie:

  - Na elk incident een grondige analyse uitvoeren om de oorzaken te identificeren.

  - Documenteer lessen en integreer deze in het verbeteringsproces.

Hoofdstuk 4: Toezicht

1: Begrijpen van de Toezichthouder

- Doel: Begrijp wie de toezichthouder is en wat hun rol is.

- Actie:

  - Volg de aankondigingen van het NCSC over welke entiteit de toezichthouder zal zijn.

  - Onderzoek de specifieke verantwoordelijkheden en bevoegdheden van de toezichthouder.

2: Voorbereiding op Toezicht

- Doel: Zorg ervoor dat uw organisatie klaar is voor toezicht en audits.

- Actie:

  - Ontwikkel en implementeer een intern beleid voor compliance met de Cyberbeveiligingswet.

  - Houd een gedetailleerde administratie bij van alle beveiligingsmaatregelen en incidenten.

  - Bereid uw personeel voor op mogelijke audits door middel van training en simulaties.

3: Samenwerking met de Toezichthouder

- Doel: Werk samen met de toezichthouder om naleving te waarborgen.

- Actie:

  - Stel een contactpersoon aan die verantwoordelijk is voor de communicatie met de toezichthouder.

  - Reageer tijdig op informatieverzoeken en volg de aanbevelingen van de toezichthouder op.

  - Voer periodieke interne reviews uit om ervoor te zorgen dat uw organisatie blijft voldoen aan de wettelijke vereisten.

4: Voorbereiding op Audits

- Doel: Bereid uw organisatie voor op mogelijke audits door de toezichthouder.

- Actie:

 - Stel een auditteam samen dat verantwoordelijk is voor het voorbereiden en begeleiden van audits.

 - Ontwikkel een interne checklist en voer periodieke interne audits uit om de naleving van de Cyberbeveiligingswet te controleren.

5: Communicatie met de Toezichthouder

- Doel: Onderhoud een open en transparante communicatie met de toezichthouder.

- Actie:

 - Wijs een vaste contactpersoon aan voor alle communicatie met de toezichthouder.

 - Houd regelmatige voortgangsgesprekken en stel vragen om duidelijkheid te verkrijgen over nalevingsvereisten.

6: Rapportage en Feedback Mechanismen

- Doel: Zorg voor tijdige en nauwkeurige rapportages aan de toezichthouder en integreer feedback in de nalevingsprocessen.

- Actie:

 - Ontwikkel gestandaardiseerde rapportagesjablonen om de naleving van de Cyberbeveiligingswet te documenteren.

 - Implementeer een feedbackmechanisme om continu verbeteringen door te voeren op basis van terugkoppeling van de toezichthouder.

7: Nalevingsaudits door Externe Partijen

- Doel: Laat externe partijen periodiek nalevingsaudits uitvoeren.

- Actie:

  - Contracteer een gerenommeerd extern auditbedrijf om jaarlijkse nalevingsaudits uit te voeren.

  - Gebruik de auditresultaten om nalevingsprocessen te verbeteren.

8: Risicobeoordeling en Mitigatie

- Doel: Voer regelmatig risicobeoordelingen uit en implementeer mitigatiemaatregelen.

- Actie:

  - Gebruik risicobeoordelingstools om potentiële risico's te identificeren en te evalueren.

  - Ontwikkel en implementeer een risicobeheersplan om geïdentificeerde risico's te mitigeren.

9: Regelmatige Rapportages aan Management

- Doel: Houd het management op de hoogte van de nalevingsstatus en incidenten.

- Actie:

  - Stel een rapportageprocedure in om regelmatig updates aan het management te geven.

  - Voorzie het management van gedetailleerde rapporten over de nalevingsstatus en eventuele incidenten.

10: Beheer van Beleidsdocumenten

- Doel: Zorg voor een centrale repository voor alle beleidsdocumenten.

- Actie:

  - Gebruik een Document Management System (DMS) om alle beleidsdocumenten, procedures en protocollen te beheren.

  - Zorg voor versiebeheer en toegangscontrole om de integriteit en veiligheid van documenten te waarborgen.

11: Regelmatige Updates van Nalevingsbeleid

- Doel: Zorg dat het nalevingsbeleid regelmatig wordt bijgewerkt.

- Actie:

  - Stel een beleid op voor periodieke herziening en bijwerking van nalevingsdocumenten.

  - Betrek alle relevante afdelingen bij de herziening om te garanderen dat het beleid up-to-date blijft met de nieuwste regelgeving en best practices.

12: Implementatie van Toezichttechnologieën

- Doel: Gebruik geavanceerde technologieën om naleving te monitoren.

- Actie:

  - Implementeer tools voor continuous monitoring en compliance management.

  - Gebruik data-analyse en rapportagetools om nalevingsgegevens te analyseren en te rapporteren aan de toezichthouder.

13: Bewustwordingsprogramma’s

- Doel: Verhoog de bewustwording over toezicht en naleving onder alle medewerkers.

- Actie:

- Ontwikkel en implementeer bewustwordingsprogramma's die medewerkers informeren over hun rol in het naleven van de Cyberbeveiligingswet.

- Organiseer workshops en trainingen om de kennis over naleving en toezicht te vergroten.

14: Samenwerking met Interne Auditteams

- Doel: Werk samen met interne auditteams om naleving te controleren.

- Actie:

- Stel een samenwerkingsplan op met interne auditteams om periodieke nalevingscontroles uit te voeren.

- Gebruik de bevindingen van de interne audits om processen en procedures te verbeteren.

15: Proactieve Voorbereiding op Toezicht

- Doel: Bereid de organisatie voor op toekomstig toezicht door regelgevende instanties.

- Actie:

- Voer proactieve nalevingscontroles uit om ervoor te zorgen dat de organisatie altijd klaar is voor inspecties.

- Zorg voor regelmatige updates van nalevingsprotocollen op basis van feedback en nieuwe regelgeving.

16: Ontwikkeling van Compliance Dashboards

- Doel: Gebruik dashboards om naleving en toezicht visueel te monitoren.

- Actie:

  - Ontwikkel en implementeer compliance dashboards die in realtime de nalevingsstatus tonen.

  - Gebruik de dashboards om snel problemen te identificeren en te adresseren.

17: Beoordeling van Beveiligingsincidenten

- Doel: Voer gedetailleerde beoordelingen uit van beveiligingsincidenten om naleving te verbeteren.

- Actie:

  - Analyseer elk beveiligingsincident grondig en documenteer de bevindingen.

  - Gebruik de bevindingen om beveiligings- en nalevingsprocessen te verbeteren.

18: Regelmatige Workshops en Trainingen

- Doel: Verhoog de kennis en vaardigheden van medewerkers door regelmatige trainingen.

- Actie:

  - Organiseer regelmatig workshops en trainingen gericht op naleving en beveiliging.

  - Zorg dat alle medewerkers op de hoogte zijn van de laatste regelgeving en best practices.

19: Gebruik van Compliance Software

- Doel: Gebruik gespecialiseerde software om de naleving te beheren en te monitoren.

- Actie:

  - Implementeer compliance management software die helpt bij het bijhouden van nalevingsstatussen en documentatie.

  - Train medewerkers in het gebruik van deze software om ervoor te zorgen dat ze effectief wordt gebruikt.

20: Stakeholder Engagement Programma's

- Doel: Betrek alle stakeholders bij het nalevingsproces.

- Actie:

- Ontwikkel programma's om de betrokkenheid van stakeholders te verhogen, zoals regelmatige updates, bijeenkomsten en trainingssessies.

- Zorg voor feedbackmechanismen zodat stakeholders hun zorgen en suggesties kunnen delen.

21: Proactieve Toezichtstrategieën

- Doel: Anticipeer op toezichtbezoeken en wees voorbereid.

- Actie:

- Voer regelmatig interne beoordelingen uit om naleving te waarborgen en mogelijke problemen te identificeren voordat een officieel toezichtbezoek plaatsvindt.

- Bereid gedetailleerde documentatie en rapportages voor om aan de toezichthouder te presenteren tijdens controles.

22: Invoering van Automatisering voor Naleving

- Doel: Verhoog de efficiëntie van nalevingsprocessen door automatisering.

- Actie:

- Implementeer geautomatiseerde compliance-tools om nalevingsactiviteiten te monitoren en te beheren.

- Automatiseer rapportageprocessen om realtime nalevingsrapporten te genereren.

23: Samenwerking met Internationale Toezichthouders

- Doel: Zorg voor naleving van internationale regelgeving en standaarden.

- Actie:

- Bouw relaties op met internationale toezichthouders en werk samen aan grensoverschrijdende nalevingskwesties.

- Implementeer best practices van internationale regelgeving om te zorgen voor wereldwijde naleving.

24: Continu Risicobeheer

- Doel: Voortdurend beoordelen en beheren van risico’s om naleving te garanderen.

- Actie:

- Implementeer een dynamisch risicobeheerprogramma dat regelmatig risico's beoordeelt en bijwerkt.

- Voer kwantitatieve risicobeoordelingen uit om prioriteit te geven aan de mitigatie van de meest kritische risico's.

25: Benchmarking tegen Industrie Standaarden

- Doel: Vergelijk nalevingsprestaties met industriestandaarden.

- Actie:

- Voer benchmarking-activiteiten uit om de nalevingsstatus van de organisatie te vergelijken met industriestandaarden en best practices.

- Gebruik de resultaten om hiaten te identificeren en nalevingsstrategieën aan te passen.

26: Deelname aan Cybersecurity Consortia

- Doel: Werk samen met andere organisaties om kennis en middelen te delen.

- Actie:

- Neem deel aan nationale en internationale cybersecurity consortia en werkgroepen.

- Deel kennis, ervaringen en bronnen om nalevingsdoelstellingen te bereiken en te verbeteren.

27: Ontwikkeling van Continuïteitsplannen

- Doel: Zorg voor de voortzetting van essentiële diensten tijdens en na een cyberincident.

- Actie:

  - Ontwikkel en implementeer business continuity plannen (BCP) die rekening houden met cyberincidenten.

  - Test en actualiseer deze plannen regelmatig om te zorgen dat ze effectief zijn en aansluiten op de nalevingsvereisten.

28: Uitvoeren van Onafhankelijke Audits

- Doel: Laat onafhankelijke derde partijen audits uitvoeren om naleving te waarborgen.

- Actie:

  - Contracteer erkende externe auditors om periodieke nalevingsaudits uit te voeren.

  - Gebruik de auditresultaten om verbeterpunten te identificeren en aan te pakken.

29: Implementatie van Correctieve Acties

- Doel: Ontwikkel en implementeer correctieve acties op basis van auditbevindingen.

- Actie:

  - Maak een actieplan om de tekortkomingen die tijdens de audits zijn geïdentificeerd aan te pakken.

  - Volg de voortgang van deze acties en voer indien nodig extra maatregelen in.

30: Continue Evaluatie en Verbetering

- Doel: Zorg voor een doorlopende evaluatie en verbetering van de nalevingsprocessen.

- Actie:

  - Stel een permanente commissie in voor naleving en verbetering, die regelmatig bijeenkomt om de nalevingsstatus te evalueren.

  - Gebruik feedback van audits, medewerkers en externe adviseurs om processen continu te verbeteren.

Hoofdstuk 5: Conclusie

- Samenvatting: Dit handboek biedt een gedetailleerde gids voor het voldoen aan de registratieplicht, meldplicht, en toezichtseisen van de Cyberbeveiligingswet.

- Aanbeveling: Blijf voortdurend op de hoogte van wijzigingen in de wetgeving en pas uw processen en procedures dienovereenkomstig aan.

-Door deze extra stappen en details te volgen, kunnen organisaties hun nalevingsprocessen verder verfijnen en versterken, waardoor ze beter voorbereid zijn op de eisen van de Cyberbeveiligingswet en hun weerbaarheid tegen cyberdreigingen verbeteren.

-Met deze uitgebreide stappen en gedetailleerde richtlijnen kunnen organisaties hun nalevingsprocessen verder versterken en een robuuste strategie ontwikkelen om aan de eisen van de Cyberbeveiligingswet te voldoen en hun cyberweerbaarheid te verhogen.

Bijlagen (verkrijgbaar op aanvraag)

- Bijlage A: Voorbeeldregistratieformulier NCSC
- Bijlage B: Checklist voor incidentmelding
- Bijlage C: Voorbeeldrapportageformulier voor de toezichthouder en CSIRT
- Bijlage D: Lijst met sector-specifieke toezichthouders
- Bijlage E: Voorbeeld van een Incident Response Plan
- Bijlage F: Opleidingsmaterialen voor Incidentrespons
- Bijlage G: Beveiligingscertificeringen en Normen
- Bijlage H: Documentbeheer en Versiebeheer Richtlijnen
- Bijlage I: Voorbeeld Escalatieprocedure
- Bijlage J: Communicatieprotocollen voor Incidenten
- Bijlage K: Samenwerkingsplannen voor Interne Audits
- Bijlage L: Crisiscommunicatieplan
- Bijlage M: Compliance Dashboard Templates
- Bijlage N: Trainingsschema’s en Workshop Materialen
- Bijlage O: Best Practices Documentatie
- Bijlage P: Rapportagesjablonen voor Aandeelhouders
- Bijlage Q: Beoordelingsrapporten van Externe Adviseurs
- Bijlage R: Data Governance Beleid
- Bijlage S: Training Programma voor Registratiebeheerders
- Bijlage T: Cyber Insurance Richtlijnen
- Bijlage U: Incidentclassificatiesysteem
- Bijlage V: Benchmarking Rapporten
- Bijlage W: Continuïteitsplannen
- Bijlage X: Onafhankelijke Audit Resultaten
- Bijlage Y: Correctieve Actieplannen
- Bijlage Z: Evaluatie- en Verbeteringsrapporten