NIS2 checklist voor KMO's

Veilig Digitaal Ondernemen helpt KMO's bij het navigeren door de complexiteit van de nieuwe NIS2 regelgeving, die ingaat op **17 oktober 2024**. Deze checklist biedt een stapsgewijze gids om ervoor te zorgen dat jouw organisatie voldoet aan de NIS2 vereisten en klaar is voor de uitdagingen van cybersecurity. Of je nu net begint met de implementatie van beveiligingsmaatregelen of bestaande processen wilt verbeteren, deze checklist ondersteunt je bij het beschermen van je netwerk- en informatiesystemen tegen cyberdreigingen.

[Template]: Wij voorzien templates voor de meeste van de documenten in deze checklist. Deze templates helpen je om snel en efficiënt aan de slag te gaan met het opstellen van beleid, procedures en andere vereiste documentatie. Bezoek onze **documentatiepagina** voor een volledig overzicht van alle beschikbare templates.

De NIS2 richtlijn begrijpen

- [ ] Lees de NIS2 regelgeving en noteer de belangrijkste punten.
*Informeer je volledig op de website van **Veilig Digitaal Ondernemen**.*

- [ ] Bepaal welke delen van de regelgeving van toepassing zijn op onze organisatie.
Identificeer specifieke vereisten en controleer welke direct invloed hebben op je bedrijfsprocessen en -systemen.

Beleid

- [ ] Schrijf een eenvoudig informatiebeveiligingsbeleid **[Template]**
Maak een document dat de belangrijkste regels en procedures beschrijft voor het beschermen van bedrijfsinformatie. Dit document moet gemakkelijk te begrijpen en te volgen zijn voor alle medewerkers.

- [ ] Maak een plan voor incident response **[Template]**
Dit plan moet beschrijven wat er moet gebeuren bij een beveiligingsincident, wie er verantwoordelijk is voor welke acties en hoe incidenten moeten worden gerapporteerd en opgelost.

- [ ] Wijs een verantwoordelijk persoon aan
Identificeer een persoon of een team binnen je organisatie dat verantwoordelijk is voor alle cybersecurity-gerelateerde activiteiten en zorg ervoor dat ze de benodigde middelen en ondersteuning krijgen.

Samen werken aan een veilige digitale toekomst

Risicobeoordeling

☐ Voer een risicobeoordeling uit: Identificeer mogelijke risico's voor onze systemen
Maak een lijst van alle mogelijke bedreigingen en kwetsbaarheden die van invloed kunnen zijn op je netwerk- en informatiesystemen. Denk aan zaken zoals malware, phishing-aanvallen en systeemstoringen.

☐ Voer een risicobeoordeling uit: Identificeer mogelijke risico's voor onze systemen **[Template]**
Stel maatregelen voor die deze risico's kunnen beperken of voorkomen. Dit kan variëren van technische oplossingen tot beleidsaanpassingen en training van medewerkers.

Technische maatregelen

☐ Netwerkbeveiliging: Installeer firewalls en zet netwerkmonitoring op
Zorg voor een stevige beveiliging van je netwerk door het installeren van firewalls en het opzetten van systemen die verdachte activiteiten kunnen detecteren en rapporteren.

☐ Toegangsbeheer: Beperk toegang tot gevoelige systemen en gegevens
Gebruik principes zoals 'least privilege' en 'need-to-know' om ervoor te zorgen dat alleen bevoegde personen toegang hebben tot kritieke systemen en gegevens.

☐ Encryptie: Implementeer encryptie voor gevoelige gegevens
Bescherm gevoelige gegevens door ze te versleutelen, zowel tijdens opslag als tijdens de overdracht. Dit helpt bij het voorkomen van datalekken.

☐ Back-ups: Stel een schema op voor regelmatige back-ups van kritieke gegevens
Zorg ervoor dat er regelmatig back-ups worden gemaakt van belangrijke gegevens en test regelmatig het herstelproces om er zeker van te zijn dat back-ups correct werken.

☐ Patching en updates: Zorg ervoor dat alle systemen up-to-date zijn
Houd alle software en systemen up-to-date met de laatste beveiligingspatches en updates om kwetsbaarheden te verminderen.

Samen werken aan een veilige digitale toekomst

Training & bewustzijn

☐ Organiseer regelmatige beveiligingstrainingen voor alle medewerkers

Plan trainingen waarin medewerkers worden geïnformeerd over de nieuwste cybersecurity-bedreigingen en hoe ze zich daartegen kunnen beschermen.

☐ Plan simulatie-oefeningen om de paraatheid van het team te testen

Voer regelmatig oefeningen uit om te testen hoe goed het team voorbereid is op een echt beveiligingsincident. Dit helpt om zwakke punten te identificeren en te verbeteren.

> *Veilig Digitaal Ondernemen organiseert evenementen zoals escape rooms en dergelijke om op een leuke manier medewerkers bewust te maken. Bekijk zeker de evenementen op de website of neem contact op om het initiatief naar jou te laten komen.*

Toezicht en rapportage

☐ Implementeer monitoring- en loggingmechanismen

Zorg ervoor dat alle activiteiten op kritieke systemen worden gemonitord en gelogd. Dit helpt bij het detecteren van ongeautoriseerde toegang en andere verdachte activiteiten.

☐ Stel een procedure op voor het rapporteren van beveiligingsincidenten **[Template]**

Maak een duidelijke procedure voor het melden van beveiligingsincidenten aan het management en, indien nodig, aan de relevante autoriteiten.

☐ Houd een logboek bij van alle incidenten, trainingen en audits **[Template]**

Registreer alle beveiligingsincidenten, trainingsevenementen en auditresultaten in een logboek voor toekomstige referentie en verbetering.