IURO ICT SERVICE AMSTERDAM

CHECKLIST

Is jouw MKB klaar voor NIS2?

Een praktische eerste check voor ondernemers en managers die grip willen op cyberweerbaarheid.

Voor MKB-teams

Praktisch toepasbaar

IURO ICT Service Amsterdam

Altijd dichtbij met ICT

Waarom deze checklist?

NIS2 vraagt om meer aantoonbare cyberweerbaarheid. Ook organisaties die niet direct onder de wet vallen, krijgen ermee te maken via klanten, leveranciers of verzekeraars. Deze checklist helpt je bepalen waar je nu staat en waar de grootste verbeterpunten zitten.

1
Maak verantwoordelijkheid expliciet

2
Bescherm toegang en identiteit

3
Test herstel voordat het nodig is

Zo gebruik je hem

Loop de onderdelen door met directie, operations en je ICT-partner. Geef elk punt groen, oranje of rood. Begin met rode punten die direct risico opleveren.

Waar IURO op let

Wij vertalen security naar duidelijke afspraken, beheerde werkplekken, zichtbare opvolging en maatregelen die passen bij de grootte van je organisatie.

1. Bestuur, toegang en herstel

Bestuur en verantwoordelijkheid

- [ ] Is duidelijk wie intern verantwoordelijk is voor informatiebeveiliging?
- [ ] Worden securityrisico's periodiek besproken op directie- of managementniveau?
- [ ] Is bekend welke systemen kritisch zijn voor de dagelijkse operatie?
- [ ] Zijn afspraken met ICT-leveranciers vastgelegd en actueel?

Toegang en identiteit

- [ ] Gebruikt iedereen multifactor-authenticatie op e-mail, Microsoft 365 en belangrijke applicaties?
- [ ] Worden accounts van vertrekkende medewerkers direct geblokkeerd?
- [ ] Zijn adminrechten beperkt tot mensen die ze echt nodig hebben?
- [ ] Is er overzicht van gedeelde mailboxen, externe accounts en gastgebruikers?

Back-up en herstel

- [ ] Worden back-ups automatisch gemaakt en periodiek getest?
- [ ] Staat minimaal een back-up los van de primaire cloudomgeving?
- [ ] Weet je hoe snel je weer kunt werken na ransomware of dataverlies?
- [ ] Zijn herstelprocedures vastgelegd in begrijpelijke stappen?

Prioriteit

Start met MFA, adminrechten, back-upcontrole en incidentafspraken. Deze basis verlaagt direct het risico en maakt vervolgmaatregelen veel eenvoudiger.

2. Incidenten en bewustwording

Incidenten en continuiteit

- ☐ Is er een eenvoudig incidentplan met telefoonnummers, rollen en eerste acties?
- ☐ Weet het team wat te doen bij phishing, datalekken of ransomware?
- ☐ Worden incidenten geregistreerd en achteraf geevalueerd?
- ☐ Zijn leveranciers bereikbaar als er buiten kantooruren iets gebeurt?

Bewustwording

- ☐ Krijgen medewerkers uitleg over phishing, wachtwoorden en veilig delen van data?
- ☐ Is er een laagdrempelige manier om verdachte e-mails te melden?
- ☐ Wordt security praktisch uitgelegd, zonder jargon?

Eerste stap met IURO

Scoor elk onderdeel met groen, oranje of rood. Begin met de rode punten die direct risico opleveren. IURO kan helpen met een compacte ICT-scan en een praktisch verbeterplan.