

Maatregel

Check

1. Inventariseer digitale activa

- Maak een lijst van alle hardware, zoals computers, servers en mobiele apparaten.
- Inventariseer alle software en applicaties die je bedrijf gebruikt.
- Identificeer gevoelige data en waar deze worden opgeslagen.
- Breng netwerkapparatuur in kaart, zoals routers en firewalls.

☐
☐
☐
☐

2. Implementeer sterk wachtwoordbeheer

- Gebruik unieke wachtwoorden voor elk account.
- Stel een minimale lengte van 12 tekens in.
- Combineer hoofdletters, kleine letters, cijfers en speciale tekens.
- Implementeer multi-factor authenticatie (MFA) waar mogelijk.
- Overweeg het gebruik van een wachtwoordmanager voor het hele bedrijf.

☐
☐
☐
☐
☐

3. Update (verouderde) software

- Schakel automatische updates in voor besturingssystemen en applicaties.
- Controleer regelmatig updates en installeer beschikbare updates.
- Stel een beleid op voor het uitschakelen van verouderde software en hardware.
- Pas kritieke beveiligingspatches zo snel mogelijk toe.

☐
☐
☐
☐

4. Breng je netwerkbeveiliging op orde

- Installeer en configureer een firewall.
- Installeer antivirus- en anti-malwaresoftware op alle apparaten.
- Gebruik endpoint detection & response (EDR) oplossingen.
- Maak regelmatig back-ups van alle kritieke data.
- Implementeer applicatie whitelisting om ongeautoriseerde software te blokkeren.

☐
☐
☐
☐
☐

Proactief werkplekbeheer



Heldere supportafspraken



Cyber security op orde



Strategisch en future-proof

Hoogwaardig IT- systeembeheer

"Op dit moment staan we op IT-gebied waar we willen staan, alles is technisch helemaal in orde. Inmiddels zitten we volledig in de cloud, met de Digital Care oplossing, combineerd met ANYBASE voor onze ERP-systemen. Dit werkt perfect."

Kees Pichal - All Safety

Maatregel

Check

5.

Beperk toegang tot het netwerk

- Gebruik een Virtual Private Network (VPN) voor externe toegang en remote werken.
- Segmenteer je netwerk om gevoelige data te isoleren.
- Beperk toegang tot het netwerk voor gasten en onbekende apparaten.

☐
☐
☐

6.

Beveilig e-mail en communicatie

- Implementeer spam- en phishingfilters.
- Gebruik e-mailencryptie voor gevoelige communicatie.
- Train medewerkers in het herkennen van phishing-pogingen.
- Overweeg het gebruik van een beveiligd berichtensysteem voor interne communicatie.

☐
☐
☐
☐

7.

Beheer toegangsrechten

- Implementeer het principe van least privilege.
- Gebruik rolgebaseerde toegangscontrole (RBAC).
- Voer regelmatig audits uit van gebruikersrechten.
- Zorg voor een gestructureerd proces voor het toekennen en intrekken van toegang.

☐
☐
☐
☐

8.

Ontwikkel een beveiligingsbeleid

- Stel richtlijnen op voor het gebruik van bedrijfsmiddelen.
- Definieer procedures voor incidentrespons.
- Creëer een acceptabel gebruiksbeleid voor medewerkers.
- Zorg voor regelmatige updates en communicatie van het beleid.

☐
☐
☐
☐

9.

Investeer in gebruikersondersteuning

- Organiseer regelmatige bewustwordingstrainingen over cyber security.
- Leer medewerkers hoe ze verdachte activiteiten herkennen en melden.
- Voer gesimuleerde phishing-tests uit om de waakzaamheid te testen.

☐
☐
☐

10.

Beveilig mobiele apparaten

- Implementeer mobile device management (MDM) oplossingen.
- Zorg ervoor dat apparaten op afstand kunnen worden gewist bij verlies of diefstal.
- Beperk de installatie van apps tot alleen goedgekeurde bronnen.

☐
☐
☐

11.

Beveilig cloud-diensten

- Kies betrouwbare en gecertificeerde cloud-providers.
- Gebruik sterke authenticatie voor cloud-accounts.
- Versleutel gevoelige data voordat je ze naar de cloud uploadt.
- Controleer regelmatig de beveiligingsinstellingen van je cloud-diensten.

☐
☐
☐
☐

Maatregel

Check

12.

Voer regelmatig security audits uit

- Plan regelmatige interne audits.
- Overweeg externe penetratietests om zwakke punten te identificeren.
- Analyseer logbestanden op ongebruikelijke activiteiten.
- Pas je beveiligingsmaatregelen aan op basis van de resultaten.

☐
☐
☐
☐

13.

Zorg voor naleving van wet- en regelgeving

- Identificeer welke regelgeving van toepassing is op jouw bedrijf (bijv. AVG).
- Implementeer de vereiste beveiligingsmaatregelen.
- Documenteer je nalevingsinspanningen.
- Overweeg het inhuren van een compliance-expert indien nodig.

☐
☐
☐
☐

14.

Bereid je voor op incidenten

- Ontwikkel een incidentresponsplan.
- Wijs verantwoordelijkheden toe aan teamleden.
- Oefen het plan regelmatig met simulaties.

☐
☐
☐

Proactief werkplekbeheer



Heldere supportafspraken



Cyber security op orde



Strategisch en future-proof

Lokale ICT-speler met korte lijnen

"Ik beveel Infodatek Group zeker aan. De korte lijnen en snelle acties maken het contact erg prettig. Ook de persoonlijke service en adviezen zijn goed. We zijn altijd op de hoogte van de voortgang door het online inzicht in de werkzaamheden. Zo weet je op elk moment precies hoe het ervoor staat!"

Alain Geubels - Colsen

Jouw IT óók naar een strategisch niveau tillen?

Walter de Kok

+31 (0)6 4630 7561

wdekok@infodatek.com

www.infodatek.com