Preview Cyber Fundamentals self-assessment Niveau 1 & 2

Hoe cyberweerbaar is uw bedrijf?

Dat gaat u nu ontdekken! Deze ‘Preview op het self-assessment’ geeft u inzicht in waar u staat en voor welk certificaat u in aanmerking komt, maar biedt tegelijkertijd ook de handvatten om te werken aan een verbeterstrategie. Zo biedt Cyber Fundamentals een haalbare, schaalbare en betaalbare manier om grip te krijgen op uw informatiebeveiliging en maken we u als ondernemer weerbaarder tegen cybercriminaliteit en de bijbehorende bedrijfsrisico’s.

Hoe werkt het?

Stap 1: In dit document vindt u 35 vragen over de huidige cybermaatregelen van uw onderneming. Elke vraag die u kunt beantwoorden met ‘Ja’ levert één punt op. Tel na het afronden van de vragenlijst alle punten bij elkaar op. Bekijk vervolgens voor welk certificaatniveau u in aanmerking komt.

Certificaat | Niveau 1

Heeft u 16 punten of meer verdient? Dan kunt u via onze website de officiële aanvraag voor het Cyber Fundamentals Certificaat Niveau 1 indienen. Met dit certificaat bent u op weg naar een goede basis voor uw informatiebeveiliging. U heeft inzicht in waar u staat en een heldere verbeterstrategie op weg naar Niveau 2.

Certificaat | Niveau 2

Heeft u 32 punten of meer? Dan kunt u een aanvraag indienen voor Niveau 2. Met dit certificaat kunt u aan uw partners, klanten en leveranciers aantonen dat u voldoet aan de 8 basismaatregelen van het Nationaal Cyber Security Centrum (NCSC), de 5 basisprincipes van het Digital Trust Center (DTC) en hun informatie bij u in veilige handen is.

Certificaat | Niveau 3 & Niveau 4

De certificaten voor niveau 3 en 4 zijn nog in ontwikkeling. Hiervoor werkt Cyber Fundamentals samen met grote werkgevers en brancheorganisaties, certificerende instanties, zzp’ers en mkb’ers, waarvoor ISO27001 de stip op de horizon is. Behaald u bij ons niveau 4? Dan bent u zo goed als klaar om op te gaan voor het ISO27001 certificaat.

Stap 2: Maak een account aan
Kunt u voldoende vragen met ‘ja’ beantwoorden en komt u in aanmerking voor een certificaat? Maak dan een account aan op de website en vraag een certificaat aan.

Stap 3: Start certificeringsproces Eigen Verklaring Cyberweerbaarheid
Dien uw officiële aanvraag in door de vragen te beantwoorden in uw accountomgeving of de vragen die noodzakelijk zijn voor het behalen van het door beoogde certificaat. U hoeft de vragenlijst niet in één keer in te vullen. Pauzeren is mogelijk. U krijgt direct een score te zien bij het afronden van de vragenlijst. Deze score correspondeert met één van de certificaatniveaus.

Stap 4: Toekenning certificaat Eigen Verklaring Cyberweerbaarheid
U ontvangt een certificaat passend bij het door u behaalde niveau en een digitaal keurmerk die u bijvoorbeeld op uw website kunt plaatsen.

Stap 5: Verlenging
Ongeveer 6-8 weken voordat uw certificaat verloopt ontvangt u van ons een melding dat uw certificaat gaat verlopen. U kunt verlengen door het certificaat voor het komende jaar te betalen en de vragenlijst opnieuw in te vullen.

Heeft u nog vragen?

Neem gerust contact op met onze helpdesk via info@cyberfundamentals.nl.

Deel I - Installeer updates

1.1 Heeft u alle software, systemen, webbrowsers in kaart gebracht? **Ja / Nee**

1.2 Heeft u een werkwijze, voor alle systemen dat u tijdig op de hoogte bent van updates? **Ja / Nee**

1.3 Installeert u updates tijdig? **Ja / Nee**

1.4 Bewaakt u of uw ICT dienst verlener, dat alle updates (automatisch of handmatig) tijdig zijn geinstalleerd? **Ja / Nee**

1.5 Indien bij een bekende kwetsbaarheid, uw leverancier nog geen update heeft; heeft u hiervoor een interne procedure, wat u dan gaat doen? **Ja / Nee**

1.6 Heeft u beleid, indien een softwareleverancier geen beveiligingsupdates meer levert, deze wordt vervangen? **Ja / Nee**

Deel II - Zorg dat elke applicatie en elk systeem voldoende loginformatie genereert

2.1 Heeft u inzichtelijk of al uw essentiële systemen en applicaties loginformatie genereert? **Ja / Nee**

2.2 Geven de logfiles duidelijke informatie? **Ja / Nee**

2.3 Worden auditlogboeken periodiek beoordeeld om afwijkingen of abnormale gebeurtenissen te detecteren die kunnen wijzen op een potentiële bedreiging? **Ja / Nee**

2.4 Zijn de logbestanden in een leesbaar en bruikbaar bestand opgeslagen? **Ja / Nee**

2.5 Heeft u de toegang tot de logbestanden beperkt? **Ja / Nee**

2.6 Weet u zeker dat de systeemtijden overal juist zijn? (denk aan verkeerde tijd, zomer/winter, tijdzones) **Ja / Nee**

Deel III – Awareness en wachtwoorden

3.1 Heeft u en hebben uw medewerkers een 'awareness-training' gevolgd? Zodat u tijdig de gevaren zult herkennen. (m.b.t. malware, phishing, CEO fraude etc..) **Ja / Nee**

3.2 Maken uw medewerkers gebruik van tweefactor authenticatie (2FA)? **Ja / Nee**

3.3 Heeft u beleid of procedure hoe medewerkers moeten omgaan met wachtwoorden? **Ja / Nee**

Deel IV - Maak regelmatig back-ups van uw systemen en test deze

4.1 Heeft u bepaald van welke data back-ups noodzakelijk is? **Ja / Nee**

4.2 Heeft u bepaald met welke frequentie back-ups worden gemaakt? **Ja / Nee**

4.3 Heeft u bepaald hoe lang u de back-ups zult bewaren? **Ja / Nee**

4.4 Heeft u een beleid of procedure hoe de back-upss worden getest? **Ja / Nee**

4.5 Maakt u gebruik van de 3-2-1 regel? (3 back-up versies van uw data, op 2 verschillende media, 1 op een fysiek andere locatie) **Ja / Nee**

4.6 Is de toegang tot de back-ups beperkt? **Ja / Nee**

Deel V – Segmenteer netwerken

5.1 Heeft u uw (thuis of bedrijfs-) netwerk in meerdere zones ingedeeld? **Ja / Nee**

5.2 Worden de verschillende zones beveiligd door een firewall? **Ja / Nee**

5.3 Is de toegang tot de verschillende Wifi netwerken gescheiden, met unieke wachtwoorden? **Ja / Nee**

Deel VI – Bepaal wie toegang heeft tot uw data en diensten

6.1 Is de logische toegang zo ingeregeld dat medewerkers alleen toegang hebben tot de data en systemen die ze nodig hebben voor hun werk? **Ja / Nee**

6.2 Heeft u een in-diensttreding procedure, waarbij de rechten worden toegekend conform het rechtenoverzicht? **Ja / Nee**

6.3 Heeft u een uit-dienst procedure, waarbij de rechten zo spoedig mogelijk op alle systemen worden ingetrokken? **Ja / Nee**

6.4 Is de toegang tot data en diensten alleen mogelijk met persoonlijke accounts? **Ja / Nee**

6.5 Controleert u met regelmaat de uitgegeven rechten, of deze conform de rechten structuur is? **Ja / Nee**

Deel VII - Versleutel opslagmedia met gevoelige bedrijfsinformatie

7.1 Zijn uw laptops, desktop pc etc, versleuteld? **Ja / Nee**

7.2 Versleuteld u uw belangrijkste data, zoals uw back-ups? **Ja / Nee**

7.3 Is uw wifi-netwerk goed ingesteld met de juiste encryptie? **Ja / Nee**

Deel VIII - Controleer welke apparaten en diensten bereikbaar zijn vanaf het internet en bescherm deze

8.1 Heeft u inzichtelijk welke IT-apparatuur gekoppeld en benaderbaar zijn vanaf het internet? **Ja / Nee**

8.2 Is de toegang van deze apparaten geminimaliseerd tot alleen noodzakelijk? **Ja / Nee**

8.3 Heeft u uw IT-apparatuur (printers, camera's etc.) in een separaat netwerk-segment geplaatst? **Ja / Nee**