



Factsheet

NIS2 Cyberweerbaarheid medewerkers

Versie 1.0, 25 november 2025

Inleiding

De NIS2 richtlijn en de Cyberbeveiligingswet (Cbw) hebben tot doel de cyberveiligheid van organisaties te versterken en de digitale weerbaarheid te vergroten.

Het vergroten van de digitale weerbaarheid van een bedrijf of organisatie is een 'mission impossible' als er niet wordt gewerkt aan de cyberweerbaarheid van de medewerkers.

Zo weten hackers vaak via social engineering of phishing een digitaal achterdeurtje te forceren en dringen op die manier binnen in de netwerken en systemen van bedrijven en organisaties.

Eén van de verplichte maatregelen uit de NIS2 en de Cbw is dat medewerkers worden getraind op het gebied van cyberbeveiliging en dat praktijken van cyberhygiëne worden toegepast.

Cyberweerbaarheid van medewerkers is voor iedere organisatie essentieel. Niet alleen omdat veel bedrijven en organisaties een schakel zijn in de toeleveringsketen van een NIS2 entiteit, maar omdat ieder bedrijf en organisatie te maken heeft met digitale dreigingen.

Kennis van cyberrisico's en cyberbeveiliging

Veel cyberincidenten starten bij een verkeerde handeling van een medewerker. Cyberweerbaarheid is mede door de snelle technologische ontwikkelingen een uitdaging die continue alertheid en aandacht vraagt.

Aanvallers weten dit en buiten dat uit door middel van een scala aan manipulatietechnieken. Op steeds geraffineerdere manieren weten ze personen te verleiden op links en bijlagen te klikken, met alle nadelige en soms desastreuze gevolgen van dien.

Medewerkers moeten bewust worden gemaakt van de cyberrisico's die constant aanwezig zijn en moeten kennis hebben van cyberbeveiliging.

Zo moeten ze weten hoe belangrijk het uitvoeren van updates is en hoe ze bedrijfsgegevens optimaal kunnen beschermen.

Niet alleen eigen medewerkers, maar ook externe medewerkers moeten getraind worden in cyberrisico's en cyberbeveiliging.

Cyberhygiëne praktijken

Cyberhygiëne ziet op het geheel aan praktijken en maatregelen om digitaal weerbaar te zijn. Iedere organisatie die digitaal weerbaar wil zijn moet beginnen met het op orde brengen van de interne cyberhygiëne.

Een goede cyberhygiëne omvat praktijken en maatregelen als

- het veilig gebruik van e-mail en internet
- software- en hardware-updates
- het wijzigen van wachtwoorden
- bescherming tegen phishing en social engineering
- medewerkers bewust maken van cyberdreigingen
- de beperking van toegangsaccounts op admin niveau
- netwerksegmentatie
- het maken van back-ups.

NIS2 entiteiten moeten ervoor zorgen dat medewerkers de basispraktijken van cyberhygiëne toepassen.

Omdat NIS2 entiteiten ook verantwoordelijkheid dragen voor de beveiliging van de toeleveringsketen, moeten ook medewerkers van toeleveranciers hierin getraind worden en moet ook binnen deze bedrijven continu aandacht zijn voor cyberhygiëne praktijken in bewustwordingsprogramma's voor medewerkers.

Gedragsverandering

Op het gebied van het vergroten van de cyberweerbaarheid bij medewerkers is aandacht voor gedragsverandering onmisbaar.

Digitale dreigingen zijn onzichtbaar, we zien ze niet, we voelen ze niet, we ruiken ze niet en we horen ze niet. We verwachten dat medewerkers alert op digitale dreigingen reageren, terwijl ons 'oerbrein' geprogrammeerd is om alleen te reageren op risico's die waarneembaar zijn.

Voor het vergroten van de cyberweerbaarheid van medewerkers is naast bewustwording en kennisopbouw, ook gedragsverandering nodig.

Het gedrag van medewerkers kan op verschillende manieren beïnvloed worden, waarbij het nabootsen van crisissituaties een zeer efficiënte manier is. Op deze manier worden digitale gevaren eerder herkend en wordt er alerter gereageerd op de gevaren.

Inspanningen om gedrag van medewerkers te veranderen zullen vooral effectief zijn als ze worden ondersteund door een leiding die cyberweerbaarheid ook serieus neemt en gedragsverandering aanmoedigt en mogelijk maakt.

Programma cyberweerbaarheid

Duthler Academy heeft een 'bewustwordingsprogramma cyberweerbaarheid' ontwikkeld, dat aangeboden wordt in een leeromgeving die bedrijfsspecifiek kan worden gemaakt.

Het bewustwordingsprogramma is bedoeld voor interne medewerkers en voor externe medewerkers die op tijdelijke basis toegang hebben tot de netwerken en systemen in uw organisatie.

Inhoud programma

In de online leeromgeving kunnen de medewerkers kennis opdoen van de verschillende cyberdreigingen zodat zij sneller een phishing e-mail of andere kwade praktijken herkennen. Ook is er aandacht voor cyberbeveiliging en voor de basispraktijken van cyberhygiëne zoals toegangsbeveiliging, software updates en veilig thuis en onderweg werken.

In de online leeromgeving kunnen de ontwikkelingen per medewerker aantoonbaar gevolgd worden. De medewerkers ontvangen een certificaat na afronding van het programma.

Aanvullend op het bewustwordingsprogramma in de eigen leeromgeving en ter bevordering van gedragsverandering van medewerkers kan Duthler Academy cursussen, workshops en oefeningen in crisissituaties op maat organiseren.

Het programma cyberweerbaarheid wordt door Duthler Academy actueel gehouden, waarbij rekening wordt gehouden met veranderingen in het dreigingslandschap en de cyberrisico's.

Cyberweerbaarheid medewerkers leveranciers

Zoals gezegd is de cyberweerbaarheid van de medewerkers van de leveranciers ook uitermate belangrijk, nu NIS2 entiteiten verantwoordelijk zijn voor de cyberbeveiliging van hun toeleveranciers.

Om in de toeleveringsketen effectief over cyberbeveiliging en cyberweerbaarheid te kunnen communiceren en over hetzelfde referentiekader te beschikken, is het advies om de medewerkers van alle bedrijven in de toeleveringsketen dezelfde opleiding te laten volgen.

Kosten cyberweerbaarheid medewerkers

Als u gebruik wilt maken van het programma cyberweerbaarheid en deze wilt aanbieden aan uw medewerkers, dan krijgt u een eigen leeromgeving. U neemt daarvoor een licentie af, die tevens toegang geeft tot online helpdeskondersteuning.

De kosten voor het gebruik van het algemeen programma bestaan uit:

- Licentie: nihil;
- € 150,- excl. BTW voor eenmalige installatie;
- € 1,- excl. BTW per persoon per maand.

De kosten voor het maken van een bedrijfsspecifieke leeromgeving worden op nacalculatiebasis in rekening gebracht.

Duthler Academy biedt binnen het programma cyberweerbaarheid voor medewerkers ook aanvullende trainingen aan die zien op gedragsverandering. Op aanvraag ontvangt u een kostenopgave.

Geïnteresseerd?

Heeft u interesse in het programma cyber-weerbaarheid voor uw medewerkers of wilt u een vrijblijvende offerte ontvangen? Neem gerust contact op met onze servicedesk en bel +31 (0) 70 392 22 09 of stuur een e-mail naar servicedesk@duthleracademy.nl.



Onze medewerkers staan klaar om uw vragen te beantwoorden. U kunt telefonisch contact opnemen. U kunt uiteraard ook een e-mail sturen.

Hoofdkantoor:

Frankenslag 137

+31 (0) 70 392 22 09

2582 HH Den Haag

servicedesk@duthleracademy.nl

<https://duthleracademy.nl/>