Cybersecurity - ondersteuning

www.vlaio.be/Cybersecurity

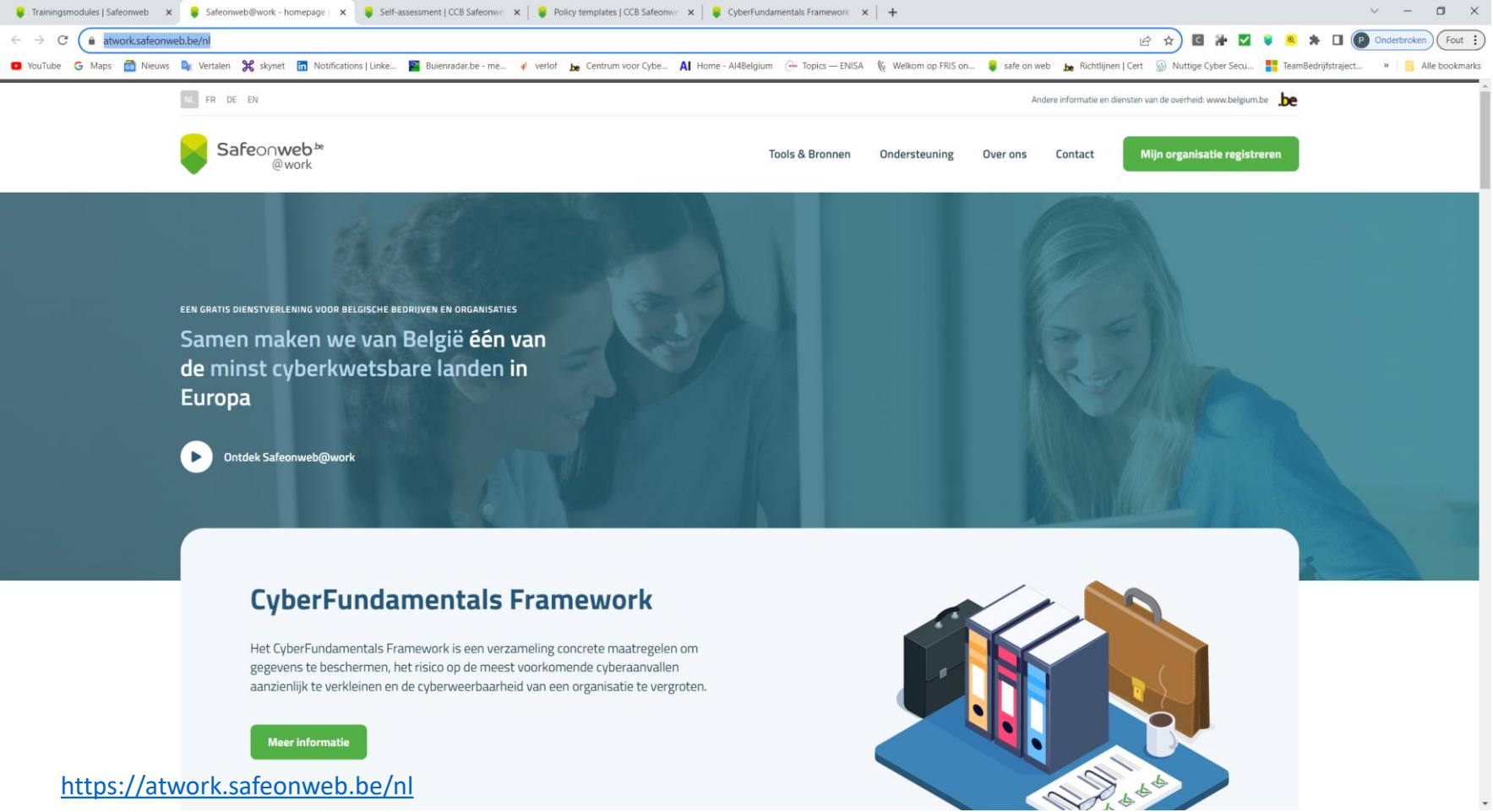
Recent nieuws…

Hacked

Booking.com

azdelta
Uw ziekenhuis.

DELTA



https://atwork.safeonweb.be/nl

https://ccb.belgium.be/news/cyfunr-2025-here

Small

Met het startersniveau **Small** kan een organisatie een eerste inschatting maken. Het is bedoeld voor micro-organisaties of organisaties met een beperkte technische kennis.

01/03/2023 · pdf

Download

Basis

Het zekerheidsniveau **Basis** bevat de standaardmaatregelen voor informatiebeveiliging voor alle ondernemingen. Deze bieden een effectieve beveiligingswaarde met technologie en processen die over het algemeen al beschikbaar zijn. Waar gerechtvaardigd, zijn de maatregelen op maat gesneden en verfijnd.

01/03/2023 · pdf

Download

Belangrijk

Het zekerheidsniveau **Belangrijk** is bedoeld om naast de gekende cyberbeveiligingsrisico's ook de risico's op gerichte cyberaanvallen door actoren met gebruikelijke vaardigheden en middelen tot een minimum te beperken.

01/03/2023 · pdf

Download

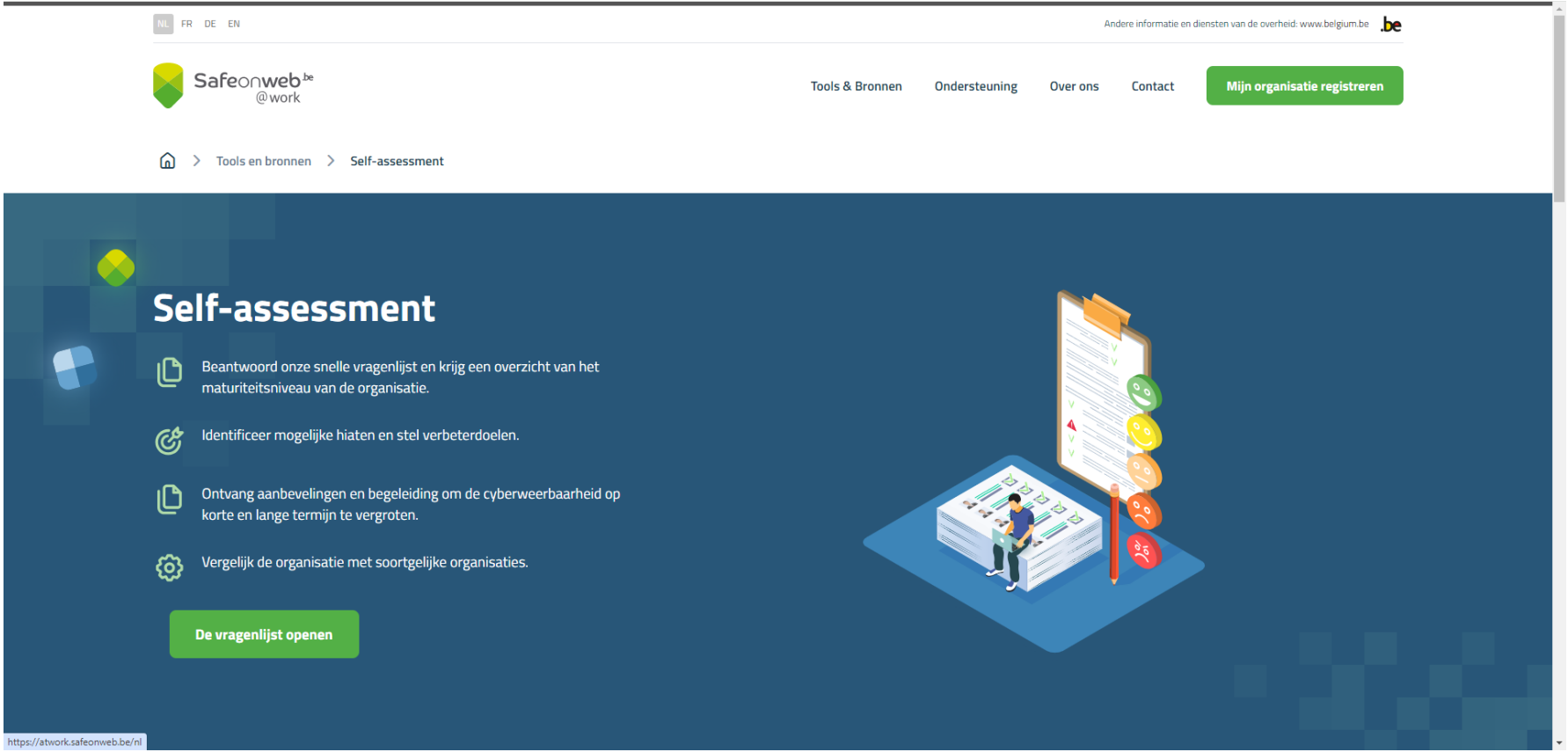
Essentieel

Het zekerheidsniveau **Essentieel** gaat nog een stap verder en is bedoeld om een antwoord te bieden op het risico op geavanceerde cyberaanvallen door actoren met uitgebreide vaardigheden en middelen.

01/03/2023 · pdf

Download

https://atwork.safeonweb.be/nl/tools-resources/cyberfundamentals-framework



https://atwork.safeonweb.be/nl/tools-resources/self-assessment

NL FR DE EN

Andere informatie en diensten van de overheid: www.belgium.be .be

Safeonweb.be @work

Tools & Bronnen | Ondersteuning | Over ons | Contact | Mijn organisatie registreren

Tools en bronnen > Policy templates

Policy templates

Het Centrum voor Cybersecurity België (CCB) biedt alle Belgische bedrijven een bibliotheek met referentiedocumenten over cyberbeveiliging

Deze referentiedocumenten zijn sjablonen van beleidsregels, instructies, inventarissen, lijsten...

Het doel is om een organisatie in staat te stellen snel en eenvoudig een cyberbeveiligingsbeleid te implementeren.

Elk model kan vrij worden aangepast, aangevuld en aangepast aan de behoeften.

https://atwork.safeonweb.be/nl/tools-resources/policy-templates

Verhoogd steunpercentage kmo-portefeuille

Verhoogd steunpercentage voor Cyberveiligheid in de kmo-portefeuille

- 35% voor MO's en 45% voor KO's (maximum steunbedrag 7.500 EUR ongewijzigd)
- Voor OPLEIDING inzake cyberveiligheid
- Van toepassing op alle dienstverleners in de kmo/p

Use case

Inarto laat verbeterde cybersecurity mee betalen door kmo-portefeuille

Bescherming tegen hackers hoeft noch een grote investering te vragen, noch ingewikkeld te zijn. Dat ervaarde Inarto architecten, een typische Vlaamse kmo met acht medewerkers.

Lees meer

Meer info op : www.vlaio.be/kmo-portefeuille

Cybersecurity-verbetertrajecten

Wat?

Steun om **extern advies** en **begeleiding** in te kopen waarmee je de cyberveiligheid van jouw onderneming duurzaam versterkt.

Je kiest uit de drie pakketten van één van de **door VLAIO geselecteerde dienstverleners**

- **START**: eerste analyse + opmaak actieplan (tussen € 7.100 en € 11.900 (excl. btw))
- **MEDIUM**: analyse + opmaak actieplan + begeleiding en advies bij oplossen beperkt aantal veiligheidsproblemen (tussen € 16.600 en € 28.600 (excl. btw))
- **PLUS**: analyse + opmaak actieplan + begeleiding en advies bij oplossen veiligheidsproblemen (tussen € 26.500 en € 39.900 (excl. btw)

Voor wie?

Voor **kmo's en maatwerkbedrijven** (50%)

en **grote ondernemingen die aan NIS2 moeten voldoen** (35%)

- die hun eerste stappen zetten op vlak van cyberveiligheid en/of kmo's met een minder complexe IT/OT-omgeving.
- met een business kritische hoeveelheid aan IT-architectuur, software of verbonden IoT-systemen.

Meer info op : www.vlaio.be/cybersecurity-verbetertrajecten

Cybersecurity-verbetertrajecten

CYBERSECURITY VLAANDEREN
BOUWEN AAN JE DIGITALE TOEKOMST

Hoe?

Stap 1	Een **onderneming** neemt zelf **contact** op met één van de 10 door VLAIO geselecteerde dienstverleners • Elk bedrijf kan hierbij zelf de dienstverlener kiezen die het best aansluit bij zijn profiel. • Partners uit VLAIO-netwerk bieden ondersteuning en verwijzen door
Stap 2	Tijdens een **intakegesprek** bepaalt de dienstverlener of een kmo in aanmerking komt voor de dienstverlening • Waar nodig kan de dienstverlener doorverwijzen naar andere instrumenten
Stap 3	De **dienstverlener** maakt in overleg met de kmo een **offerte** op en bezorgt deze samen met '**aanvraagdocument**' aan VLAIO
Stap 4	**VLAIO** keurt de aanvraag goed (doorlooptijd van circa 7 dagen)
Stap 5	De dienstverlening kan van **start** gaan • Na rapportering door de dienstverlener betaalt VLAIO zijn aandeel aan de dienstverlener

Cybersecurity

Vandaag is elk bedrijf – groot of klein - een mogelijk doelwit voor cybercriminelen. Zorg daarom dat jouw bedrijf digitaal even goed beveiligd is als je voordeur. Op deze pagina's lees je hoe je een cyberaanval voorkomt, waarom investeren in cyberveiligheid loont, wat je moet doen als je getroffen wordt door een cyberaanval, en bij wie je terecht kan met jouw vragen. Je krijgt ook een overzicht van interessante opleidingen en webinars.

Wordt het jou te complex? Laat je dan begeleiden. Spreek je IT-partner aan of neem een cybersecurity expert onder de arm. VLAIO komt tussen in de kosten via verschillende subsidies.

Vind nu een opleiding

› **Cybersecurity verbetertrajecten**

Steun, advies en begeleiding om je op weg te helpen

› Waarom inzetten op cybersecurity?

Door de toegenomen digitalisering van de economie en de samenleving lopen Vlaamse bedrijven meer dan ooit het risico om gehackt te worden.

› Advies, begeleiding en financiële steun

Een sterk cybersecuritybeleid wekt vertrouwen op bij klanten en leveranciers. Ontdek het aanbod aan advies en begeleiding en financiële steun.

› Zelf aan de slag met cyberveiligheid

Je kan een aantal basisacties nemen om de cyberveiligheid van je onderneming te verhogen.

› Cyberincident, volg dit stappenplan

Reageer snel en juist als een cyberincident zich voordoet. We zetten de belangrijkste stappen op een rijtje.

Gratis tools

Je kan zelf al van start gaan om de cyberveiligheid van je onderneming te verbeteren en een cybersecurityplan vorm te geven. Maak hierbij zeker gebruik van de gratis templates, tools en informatiebronnen van het Safeonweb@work platform van het Centrum voor Cybersecurity Belgium (CCB).

- Via het Safeonweb@work platform van het CCB zijn onder andere volgende diensten beschikbaar:
  - Met de self-assesment tool toetst je het maturiteitsniveau van je organisatie.
  - Via de Quick Wins vind je tips en korte stappenplannen hoe je basisacties zelf kunt implementeren
  - Policy templates: sjablonen om je informatiebeveiligheidsbeheer te implementeren
  - Video's en Webinars om jezelf en personeel de basisprincipes aan te leren
  - Mogelijkheid om je onderneming te registeren zodat je waarschuwingen ontvangt voor potentiële bedreigingen en kwetsbaarheden in je netwerk.
  - Een internetbrowserextensie die de mate van vertrouwen meet die je kunt hebben in de websites die je bezoekt.
  - Een Quick Scan Report-service die een gratis risicobeoordelingsrapport geeft over de cyberveiligheid binnen je organisatie.
- Buyer's guide: een handig overzicht van vragen die je zeker aan jouw softwareleveranciers moet stellen

Volgende stappen

Wil je je cybersecurity maturiteit nog verder verhogen? Doe dan een beroep op een gespecialiseerde dienstverlener. Deze kijkt verder dan het IT-gedeelte, staat je bij om je cyberveiligheidsbeleid op punt te zetten en introduceert waar nodig de laatste nieuwe technologieën. Via een verhoogd steunpercentage van de kmo-portefeuille voor cybersecurity of een cybersecurity verbetertraject kan je een dienstverlener inhuren.

Jouw kennis verder vergroten?

Neem een kijkje in de eventkalender van VLAIO. Je vindt er alle activiteiten rond cyberveiligheid die partners uit het VLAIO-netwerk organiseren. Surf zeker ook eens naar Cybersecurity Bites. Hier vind je artikels op maat van ondernemingen en wordt het cybersecurity jargon je met bits en bites hapklaar geserveerd.

Cyberincident? Zo reageer je

Overzicht cybersecurity

Cyberincident? Zo reageer je

Wat als je getroffen wordt door een cyberaanval?

Een cyberaanval kan ernstige gevolgen hebben voor je bedrijf of organisatie. Je reputatie krijgt een stevige deuk en het brengt ook ernstige financiële gevolgen met zich mee. Volg deze stappen als je getroffen wordt door een cyberaanval.

1 Licht de verantwoordelijke voor het cybersecuritybeleid onmiddellijk in

Cybercriminelen bereiden een cyberaanval grondig voor. Ook de oplossing moet daarom methodisch zijn. Het beheer van een crisis moet op het hoogste niveau van de organisatie plaatsvinden. Hoe sneller de juiste mensen betrokken zijn, hoe beter de gevolgen van het incident beperkt kunnen worden.

Verwittig daarom meteen de collega die verantwoordelijk is om als eerste actie te ondernemen bij een cyberaanval. Die collega activeert het crisisbeheerteam en brengt iedereen die jouw IT-systemen beheert meteen op de hoogte van de infectie zodat alle aangetaste computers, machines en servers van het netwerk ontkoppeld kunnen worden. Ontkoppel ook externe harde schijven om verdere infectie te voorkomen.

2 Activeer een crisisbeheerteam en zorg vooraf voor een business continuity plan

Tijdens het beheer van de crisis zijn de acties op de verschillende betrokken gebieden cruciaal - technisch, HR, financieel, communicatie, juridisch etc.. Het crisisbeheerteam moet toezien op de acties die genomen moeten worden op elk gebied tijdens de crisis. Gevoelige communicatie over de evolutie van het incident moet via een afzonderlijk en beveiligd kanaal gebeuren.

Als je beschikt over een incident response plan en/of business continuity plan zal het

Ondernemersverhalen

Thema: - Cybersecurity

13 feb 2026

Pentesten op het tempo van software

Jaarlijkse pentests missen het tempo van moderne software. Met innovatieve startershulp van VLAIO maakt Aikido continuous pentesting schaalbaar.

› Lees meer

5 dec 2025

Oost-Vlaamse Bouwmaterialen zet structureel in op cyberveiligheid

Na een cyberincident besloot Oost-Vlaamse Bouwmaterialen hun cyberveiligheid structureel te versterken via een cybersecurity verbetertraject.

› Lees meer

20 nov 2025

Brouwerij Vanhonsebrouck versterkt digitale weerbaarheid met VLAIO en ConXioN

De brouwerij van Kasteelbier zette een grote stap naar een beter beveiligde digitale toekomst via een cybersecurity verbetertraject.

› Lees meer

14 feb 2025

CGK Group versterkt digitale veiligheid

CGK Group versterkt digitale veiligheid met Savaco. Ontdek hoe ze hun cybermaturiteit verbeterden en medewerkers bewust maakten van cyberrisico's.

14 feb 2025

INNI Group wapent zich tegen cyberdreigingen

Ontdek hoe INNI Group samen met Soteria Cybersecurity en VLAIO slimme strategieën ontwikkelt om zich te beschermen tegen cyberdreigingen.

29 nov 2024

Innovatieve phishing-simulaties

Op zoek naar een tool die je team phishing-e-mails helpt herkennen? OutKept ontwikkelde een platform dat bedrijven helpt om phishing te bestrijden..

Meer info

www.vlaio.be/cybersecurity

Contactpersonen:

patrick.hauspie@vlaio.be

Jeroen.fiers@vlaio.be

Ben je leergierig of voel je de noodzaak om je kennis over cyberveiligheid te vergroten? Surf dan zeker ook eens naar cybersecurity-bites.be