Cyberfort Antwerpen

Onze samenleving, met alle private en publieke actoren, is de afgelopen jaren in ijltempo getransformeerd naar een wereld waarin digitale dienstverlening het 'nieuwe normaal' is. Ook de burger is, in zijn relatie met lokale, regionale en federale overheden, steeds veeleisender geworden in wat hij verwacht aan digitale diensten. Deze toegenomen digitalisering heeft echter geleid tot een verhoging van het risico op verstoring door cybersecurity-incidenten.

Het project CyberFort Antwerpen heeft als doel om een veilige en betrouwbare digitale omgeving op te bouwen, waarin inwoners, bedrijven en instellingen met vertrouwen kunnen wonen, werken en ondernemen. Cyberfort Antwerpen zet zich in voor het creëren van een veerkrachtige digitale omgeving en een goed voorbereide organisatie die maximaal bestand is tegen huidige en toekomstige cyberdreigingen. Het ultieme doel van dit cybersecurity programma is het maximaal beheersen van de cyberrisico's voor de organisatie en de interne en externe gebruikers.

Hierbij zal ingezet worden op de drie belangrijkste factoren om dit te bereiken:

- Mensen (medewerkers en burgers): Mensen vormen de eerste verdedigingslinie in een cybersecurity programma. Ze kunnen potentiële dreigingen herkennen en melden, zoals phishing-pogingen of verdachte activiteiten. Echter, zonder de juiste training kunnen ze ook de zwakste schakel zijn. Bewustmaking en opleiding rond cybersecurity is dus cruciaal om menselijke fouten die tot beveiligingsinbreuken kunnen leiden, te minimaliseren.
- Processen: Goed gedefinieerde en geïmplementeerde processen zijn essentieel voor een effectief cybersecurity programma. Ze bieden een gestructureerd kader voor het reageren op incidenten, het bijwerken van software, het beheren van gebruikerstoegang en vele andere taken. Processen zorgen ook voor consistentie en reproduceerbaarheid, wat helpt bij het onderhouden van de beveiligingsstandaarden over tijd.
- Technologie: Technologie is een krachtig hulpmiddel dat gebruikt wordt om systemen en gegevens te beschermen. Het omvat alles, van basisbeveiligingssoftware zoals antivirusprogramma's en firewalls, tot geavanceerde oplossingen zoals intrusion detection systems en encryptietools. Technologie kan helpen bij het automatiseren van beveiligingstaken, het detecteren van abnormale activiteiten en het beveiligen van gevoelige informatie tegen diverse dreigingen.

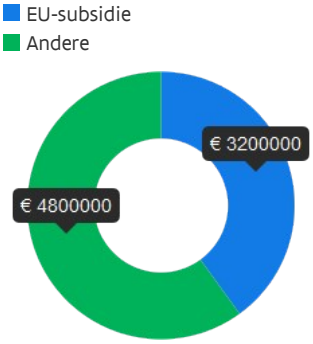
De projectoutput omvat een veilige omgeving voor honderdduizenden gebruikers, de werkwijze om dit op te zetten en te onderhouden en de best practices waaruit anderen kunnen leren.

Cyberveiligheid is voor alle Vlaamse lokale besturen een reële bedreiging. Mogelijke problemen hebben een zeer zware impact op de externe dienstverlening en interne werking. Met dit project wil de stad Antwerpen een belangrijke stap voorwaarts zetten en een trekkersrol in Vlaanderen opnemen. Het project zal

Medegefinancierd door de Europese Unie

Financiële info

Totale projectkost: € 8.000.000



Partners

Stad Antwerpen - 915

Periode

01-09-2023 tot 31-08-2026

Thema

digitalisering

inzichten en resultaten opleveren die ook door andere steden en gemeenten kunnen meegenomen worden bij de uitbouw van een cyberveiligheidsbeleid.

Prioriteit

Digitalisering