Vlaanderen
is ondernemen

DIGITALISERING

Maak van cyberveiligheid een prioriteit voor jouw kmo

VLAIO

vlaio.be/cybersecurity

Inhoud

Verantwoordelijk uitgever:
Mark Andries
Koning Albert II-laan 35 bus 12
1030 Brussel

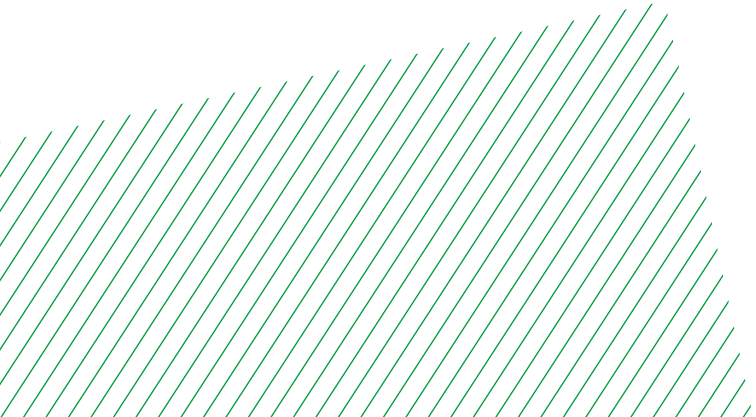
D/2022/3241/265

Versie mei 2023

Waarom inzetten op cybersecurity?

Met een cybersecuritybeleid op maat ben je beter gewapend tegen een mogelijke cyberaanval

Iederéén is vandaag een mogelijke prooi voor cybercriminelen. Zowel kleine kmo's als grote multinationals in eender welke sector kunnen op een dag geconfronteerd worden met een cyberaanval. Cybersecurity is daarom onmisbaar geworden om de continuïteit van de bedrijfsvoering te garanderen.



Waarom cybersecurity?

Cyberaanvallen richten financiële schade én reputatieschade op langere termijn aan bij bedrijven. Ze slaan een deuk in het vertrouwen bij klanten en leveranciers. Redenen genoeg om je te wapenen tegen cyberveiligheidsrisico's.

Cybercriminelen zetten een combinatie van strategieën in om toegang te krijgen tot bedrijfsnetwerken, en worden daarbij steeds inventiever. In een digitaal geconnecteerde economie kunnen ze een sneeuwbaleffect veroorzaken. Daarom heeft élke onderneming nood aan een cybersecuritybeleid op maat, en is cybersecurity een topprioriteit voor de Vlaamse overheid. De impact van een cyberincident zal immers altijd kleiner zijn bij een goed voorbereide onderneming.

HOEVEEL KOST EEN DAG STILSTAND?

Stel dat je kmo het slachtoffer wordt van een cyberaanval, welke schade zou je dan lijden? Schrijf de antwoorden neer en bespreek ze met je management.

- **Hoe lang draait je bedrijf verder eens IT onbereikbaar wordt?**
- **Hoeveel kost een dag stilstand?**
- **Heb je contracten met boeteclausules?**
- **Hoeveel aan boetes zou je moeten betalen als klantgegevens gestolen worden?**
- **Hoeveel zou het kosten om te herstarten en de gehackte data en systemen te herstellen?**
- **Hoeveel van je huidige klanten zullen niet meer bij je kopen na een hacking?**
- **Werk je voor ondernemingen die het cyberrisico van de samenwerking willen inschatten via cybersecurity-vragenlijsten?**

Steeds meer gevaar

Door de toegenomen digitalisering van de economie en de samenleving lopen Vlaamse bedrijven meer dan ooit het risico om gehackt te worden. Bijna 1 op 8 van de Vlaamse bedrijven werd afgelopen jaar slachtoffer van een cyberaanval. 40% van de kleine kmo's werd in 2021 geconfronteerd met onbruikbare ICT-systemen door cyberaanvallen Tijdens piekperioden verwijderen telecomoperatoren tot 2 miljoen phishingsms'en per dag in ons land. Ook jouw medewerkers ontvangen misleidende berichten via mail, sms en telefoon. Deze leiden soms tot een hacking, het verspreiden van virussen, het stelen en gijzelen van data via ransomware en het stilleggen van productiemachines.

Het kan elke kmo overkomen

Tegenover elke grote cyberaanval die de media haalt, staan tientallen aanvallen bij kleinere bedrijven. Die springen minder in het oog, maar de impact op de onderneming is minstens even groot.

"Iederéén is vandaag een mogelijke prooi voor cybercriminelen. Zowel kleine kmo's als grote multinationals, in eender welke sector."

Patrick Hauspie - Bedrijfsadviseur VLAIO

Cyberveiligheid als verkoopstroef

Cybersecurity is steeds vaker een belangrijke verkoopstroef. Een sterk cybersecuritybeleid wekt immers vertrouwen bij klanten en leveranciers. Het zorgt voor businesscontinuïteit en risicomanagement en geeft je onderneming veerkracht en een professionele uitstraling. Onmisbaar voor een toekomstgerichte onderneming. Bewijzen dat je cyberveilig bent, dat je oplossingen veilig zijn en je data van klanten veilig verzamelt, bewerkt en bewaart, wordt voor steeds meer kmo's essentieel om contracten af te sluiten. Ook bij de aankoop van een digitale tool of dienst, is het belangrijk de cyberveiligheid hiervan kritisch te onderzoeken.

Stel een cybersecurityplan op

Cyberveiligheid gaat verder dan technische oplossingen zoals een firewall, een antivirusprogramma en back-ups. Er is ook een procesmatige kant, met mensen als één van de zwakke schakels. Hoe bouw je dit proces op? Hoe creëer je een cultuur van cyberveilig handelen? Welke stappen doorloop je bij een cyberaanval? Dit bepaal je allemaal in een cybersecurityplan.

Elke Vlaamse onderneming heeft nood aan een sterk onderbouwd plan van aanpak op maat. Zo'n strategie integreert, naast de noodzakelijke technologische oplossingen, cyberveilig handelen in de alledaagse werking van het bedrijf. Bovendien stelt het cybersecurityverantwoordelijken in staat om meteen te handelen bij een cyberdreiging of –aanval. Maar… in de praktijk hebben nog te weinig ondernemingen zo'n plan. De financiële steun en begeleiding van VLAIO kunnen je helpen het cybersecuritybeleid van je onderneming op punt te stellen.

De app van FibriCheck spoort hartritmestoornissen op:

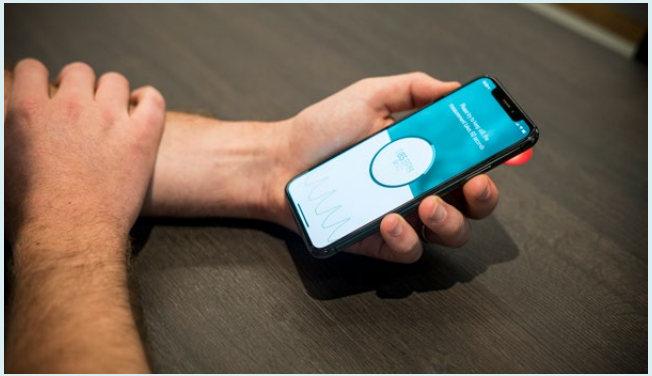
“Cyberveiligheid is extreem belangrijk voor ons”

De Limburgse scale-up FibriCheck is de wereld aan het veroveren met zijn app om hartritmestoornissen te detecteren. Gevoelige medische data van gebruikers beschermen staat bovenaan hun agenda. “Je moet van meet af aan voluit inzetten op cyberveiligheid, of je zingt het in de wereld van de digitale gezondheidszorg niet lang uit”, zegt Jo Van der Auwera, Chief Compliance Officer bij FibriCheck. Daarom volgde het bedrijf een cybersecurity verbetertraject.

FibriCheck maakt het mogelijk om zelf hartritmestoornissen op te sporen, door simpelweg je vinger op de camera van je smartphone te plaatsen. “Cyberveiligheid is extreem belangrijk voor ons”, benadrukt Jo Van der Auwera. “Digitale gezondheid is dé trust business bij uitstek. Gebruikers vertrouwen ons hun medische data toe en ze verwachten terecht dat wij daar zorgvuldig mee omspringen en die niet te grabbel gooien.”

Hoewel FibriCheck al fors investeerde in cyberveiligheid, is er altijd marge om het nog beter te doen. Cybersecurity specialist CRANIUM zette voor FibriCheck een verbetertraject op om de cybersecurity naar een nog hoger niveau te tillen. Zo'n verbetertraject verloopt in drie fases: eerst de analyse van de huidige situatie en maatregelen, dan een concreet verbeterplan met prioriteiten en met het mappen van acties, en tenslotte de roll-out van die verbeteracties. VLAIO kwam tussen voor 45% van de kost.

Door de digitalisering van de economie ben je als onderneming op veel meer plekken kwetsbaar, zelfs op afstand. Het besef dat cybercriminelen een heel bedrijf plat kunnen leggen via één smartphone of één sensor ontbreekt vaak. Jo van FibriCheck vertelt: "Eén lek kan een enorme impact hebben op de continuïteit van FibriCheck, dus we moeten altijd en overal het zekere voor het onzekere nemen. Better safe than sorry. Bij elk plan vertrekken we van het worst case scenario. Wat is het ergste dat ons kan overkomen? Dat absolute rampscenario is de leidraad. Daar moeten we ons tegen wapenen, daar leggen we de lat. Cyberveiligheid is een integraal en onmisbaar onderdeel van het veiligheidsbeleid."



"Belangrijk is dat het verbetertraject niet alleen inzoomt op technologie, al onze medewerkers moeten doordrongen zijn van het belang van cyberveiligheid. We zijn voortdurend nieuwe mensen aan het onboarden, we leren hen hoe ze risico's detecteren en vermijden. We organiseren voor iedereen halfjaarlijkse trainingen, onze security officer legt tussendoor ook mensen op de rooster als ze onvoorzichtig zijn. In het verbetertraject van VLAIO zit ook standaard e-learning en we krijgen ook een phishing training om pogingen te herkennen en af te blokken."

Investeren in cybersecurity doe je niet alleen! Ontdek de financiële steun

Denk je aan investeren in cybersecurity? De return on investment is helemaal voor jou en je onderneming! En de investering? Die doe je niet alleen! Ontdek hier welke financiële steun je kan helpen.

Kmo-portefeuille voor advies en opleiding cybersecurity

Wil je jouw personeel opleiden rond cybersecurity? Of zoek je kwaliteitsvol advies om een cybersecurityplan op te stellen? Voor beperktere cybersecurity trajecten kan je beroep doen op de kmo-portefeuille. Je krijgt als kleine of middelgrote onderneming een hoger steunpercentage voor het inkopen van advies en opleiding rond cybersecurity.

VOOR WIE: Vlaamse kmo's of beoefenaars van vrije beroepen.

VOOR WAT: Voor de aankoop van diensten die de kwaliteit van je onderneming verbeteren. Concreet zijn dat opleidingen en adviesdiensten die je helpen met het cybersecurityplan van je bedrijf.

HOEVEEL SUBSIDIE: Voor cybersecurity krijgen kleine ondernemingen een hogere tussenkomst van 45%. Middelgrote ondernemingen: 35%. Tot maximaal € 7.500 per jaar.

Cybersecurity verbetertrajecten

Wil je de cyberveiligheid van je onderneming op een duurzame manier verbeteren? Krijg je graag meer vat op de kwetsbaarheden van je bedrijf? Heb je nog geen strategie om de cyberveiligheid van je onderneming te verhogen? Dan is een cybersecurity verbetertraject iets voor jou! De acht door VLAIO geselecteerde dienstverleners ondersteunen kmo's en maatwerkbedrijven bij het duurzaam versterken van hun cyberveiligheid.

"Als kmo hebben we niet alle kennis in huis. Bij het cybersecurity verbetertraject van VLAIO vonden we een externe expert die in nauwe samenwerking met onze IT-partner het volledige proces aanpakt."

Peter van Vooren, Head of digital transformation bij Remedus

VOOR WIE: Vlaamse kmo's en maatwerkbedrijven.

VOOR WAT: inkopen van extern advies en begeleiding voor cyberveiligheid.

3 paketten:

- START: eerste analyse + opmaak actieplan
- MEDIUM: analyse + opmaak actieplan + begeleiding en advies bij oplossen beperkt aantal veiligheidsproblemen
- PLUS: analyse + opmaak actieplan + begeleiding en advies bij oplossen veiligheidsproblemen

HOEVEEL SUBSIDIE: 50% steun op trajecten tussen de € 9.000 en € 35.000 (exclusief btw).

Innovatiesteun voor onderzoek & ontwikkeling

Koester je plannen om een nieuwe digitale oplossing te realiseren? Geef dan van bij de start voldoende aandacht aan cyberveiligheidsaspecten. Is je bedrijf bezig met het uitbouwen van een nieuwe cyberveiligheidsoplossing of het versterken van de onderzoeks- en ontwikkelingsactiviteiten rond digitalisering of artificiële intelligentie? Via een ontwikkelings- of onderzoeksproject krijg je van VLAIO een financieel duwtje in de rug.

VOOR WIE: Ondernemingen, non-profitorganisaties en publiekrechtelijke organisaties die een nieuwe technologie ontwikkelen waarvoor nieuwe kennis nodig is, die processen of diensten doordacht verbeteren, of een prototype bouwen of een pilootfase doorlopen.

VOOR WAT: Voor personeels- en andere kosten gerelateerd aan het project.

HOEVEEL SUBSIDIE: 25 tot 60% van de projectbegroting met minimum € 25.000 en maximaal € 3 miljoen.

Surf naar vlaio.be/cybersecurity voor meer informatie!

Advies en begeleiding

Wil je advies en begeleiding rond cybersecurity? Maak dan kennis met interessante advies- en begeleidingstrajecten.

VLAIO bedrijfsadviseurs

Heb je ambitieuze digitaliseringsplannen en wil je het aspect cyberveiligheid hierbij niet uit het oog verliezen? Dan helpen de VLAIO bedrijfsadviseurs deze waar te maken. Zij gidsen je naar de juiste kennis, partners en financiële hefbomen en brengen je in contact met cybersecurity-knowhow die specifiek voor jouw bedrijf relevant is. Denk aan private aanbieders, kennisinstellingen, strategische- en collectieve onderzoekscentra en intermediaire organisaties zoals Voka, UNIZO, Agoria ...

Maak een gratis afspraak via vlaio.be/afspraak

"Cybersecurity experts detecteren de grootste noden en kunnen prioriteiten naar voor schuiven."

Jeroen Fiers, VLAIO adviseur

Experten uit het VLAIO Netwerk

Weet je niet goed hoe te starten met een betere cyberveiligheid of wil je zelf meer te weten komen over wat cyberveiligheid inhoudt? Zoek je advies, coaching of een lerend netwerk van bedrijven die voor dezelfde uitdagingen staan? Wend je dan tot de partners uit het VLAIO Netwerk. Zij sensibiliseren, adviseren en informeren ondernemers over het belang van cyberveiligheid. Ze voorzien coaching en begeleiding rond de aanpak van cyberveiligheid in de eigen onderneming. Je kan bij hen terecht voor infosessies, masterclasses, workshops, opleidingen, netwerking, begeleiding ...

Ontdek alle initiatieven via vlaio.be/expertisedatabank

Blikopener hogescholen

Zoek je praktisch toepasbare kennis en projecten rond AI en cybersecurity? Via het project Blikopener verspreiden 10 Vlaamse hogescholen hun kennis naar bedrijven, non-profit organisaties, gemeenten, steden, OCMW's en onderwijsinstellingen. Elke ondernemer, starter of prestarter die via praktijkgericht onderzoek een oplossing zoekt voor een concreet probleem, kan bij dit platform aankloppen. Blikopener organiseert eerstelijnsadvies, ondersteunt je bij de vraagstelling van het probleem en brengt je in contact met een aantal geschikte partijen om oplossingen te ontwikkelen.

blikopener.vlaanderen

Proeftuin Innovatieve cyberbeveiliging voor industrie 4.0

Maakt je bedrijf gebruik van data- en geconnecteerde machines? Dan is beveiliging een must! De proeftuin Innovatieve cyberbeveiliging voor industriële bedrijven in de maakindustrie creëert demo's voor bedrijven die willen werken aan een doordacht cyberveiligheidsbeleid. Hier ontdek je alle do's en don'ts op het vlak van cyberbeveiliging. Inclusief de laatste nieuwe trends zoals de inzet van artificiële intelligentie als wapen tegen cyberaanvallen. Ook organiseert deze proeftuin workshops, infosessies en demo's op maat van verschillende doelgroepen.

vlaio.be/industrie40

Cybersecurity-bites

Ben je leergierig of voel je de noodzaak om bijvoorbeeld je kennis over ransomware of opkomende cybertechnologieën te vergroten? Surf dan naar cybersecurity-bites.be. Dit initiatief van Vlaamse universiteiten en hogescholen geeft professionals en onderzoekers toegang tot opleidingen en nieuwe artikels rond cyberveiligheid.

cybersecurity-bites.be

Cybersecurity? Dat is voor mij een logisch onderdeel van onderzoek en ontwikkeling

Geen product zonder cyberbeveiliging. Tijdens de ontwikkeling van de plugin Ativo Programs, een programmamanagementtool voor softwareteams, schonk ondernemer Edwin Rozie meteen de nodige aandacht aan cyberveiligheid. De plugin overtuigde intussen onder meer twee bedrijven uit de Fortune 500. Ativo Programs kreeg steun via een VLAIO-ontwikkelingsproject.

Plugin voor Jira

Ativo Programs is een plugin voor Jira, de populairste programmamanagementtool voor software teams. Edwin Rozie legt uit: “Vergelijk Jira met de bekende tools voor projectbeheer Trello of Notion. Ik bouw hier nog een laag boven die op een geconsolideerd bord linken tussen de verschillende borden toont. Als Jira teams van vijf tot tien personen helpt, bedient mijn tool tien van die teams.” Ativo Programs focust vooral op development-teams in grote bedrijven, maar kan ook ingezet worden

op omvangrijke infrastructuurprojecten, of voor een bedrijf dat besluit een nieuwe strategische richting in te slaan. “We onderscheiden ons van de anderen door onze focus op Jira, de methodologie die we ondersteunen, en het visuele. Wij kiezen grafieken in plaats van tabellen, of rode en groene indicatoren in plaats van tekst.”

Cybersecurity van in het begin

Al in het eerste prototype dat Edwin in 2019 lanceerde, zat cyberveiligheid ingebakken. “Ativo Programs verzamelt vertrouwelijke informatie van grote ondernemingen. Wetende dat hackers vaak via kleine leveranciers grote ondernemingen binnendringen, wilde ik dit risico niet lopen”, zegt de ondernemer. “Daarom maakt cybersecurity van in het begin een normaal deel van mijn onderzoek en ontwikkelingen uit.”

Tegelijkertijd vragen potentiële klanten naar zijn security policy. Ze willen weten welke maatregelen het jonge bedrijf neemt en hoe het omgaat met cybersecurity . “De twee behaalde cybersecurity certificaten van Atlassian, wat het bedrijf achter Jira is, geven mijn prospecten en klanten vertrouwen.”

Ethische hackers

Edwin nodigde 300 ethische hackers uit om kwetsbaarheden te zoeken in zijn gloednieuwe software. “Ik loofde mooi prijzengeld uit. En dus hebben deze ethische hackers alle middelen ingezet. Ze hebben een paar kwetsbaarheden aangetoond, maar geen enkele is binnengeraakt in de software”, blikt Edwin tevreden terug op de cybersecurity test. “Ik vond dat mijn IT-infrastructuur moest kunnen weerstaan aan state-of-the-art aanvallen met alle moderne aanvalstechnieken. Want de complexiteit en snelheid van aanvallen zijn uitdagend vandaag.”

Begeleiding en steun van VLAIO

In 2021 diende Edwin een dossier voor een ontwikkelingsproject in bij VLAIO. Bedrijfsadviseur Bruno Van De Casteele hielp Edwin om het dossier op te stellen. “Hij bekeek mijn dossier kritisch, vroeg bijkomende informatie en uitleg en hielp me het zo verbeteren. Het ontwikkelingsproject werd goedgekeurd kort nadat ik het indiende”, zegt Edwin. De steun helpt hem om de eerste voltijdse ontwikkelaar aan te werven en een derde versie te bouwen.

vlaio.be/cybersecurity

info@vlaio.be

Download of bestel deze brochure