CYBERBEVEILIGING - BELGISCHE MICRO-ONDERNEMINGEN EN KMO'S

JAARLIJKSE BAROMETER

2024

SKYFORCE CYBER SECURITY

METHODOLOGIE

Jaarlijkse barometer 2024

Deze vijfde Skyforce-barometer is gebaseerd op bezoeken en individuele interviews met 3.286 Belgische bedrijven, die gedurende het hele jaar 2023 zijn uitgevoerd.
Onze adviseurs hebben rechtstreeks interviews afgenomen met de managers van deze bedrijven, die in wezen micro-ondernemingen zijn met minder dan vijf werknemers.
De Skyforce-barometer is de grootste enquête over cyberbeveiliging in België bij deze categorie bedrijven.

Mathieu Lardinois

Co-Founder
Marketing & Customer Care Director

"In 2023 hebben onze experts nauwgezet werk verricht door meer dan 3.200 ondernemers in België te auditeren. Deze aanpak biedt een uniek perspectief op de uitdagingen en kansen op het gebied van cybersecurity binnen kleine en middelgrote ondernemingen."

BELANGRIJKSTE PUNTEN 2024

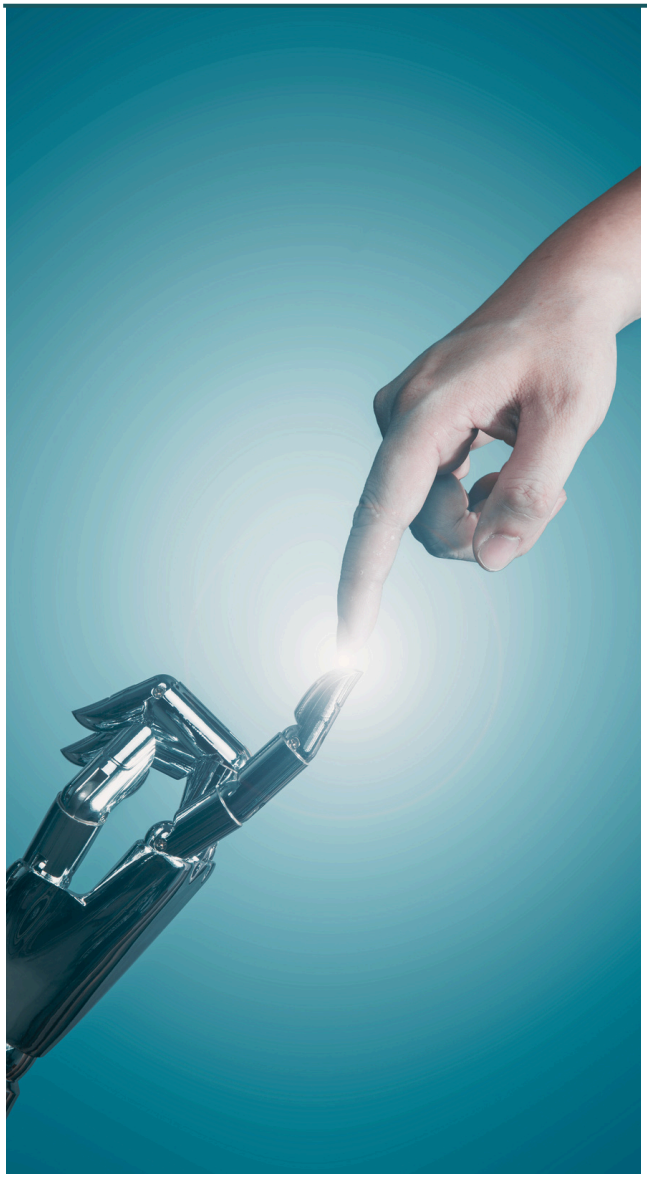
AI MET DUBBEL SNIJVLAK

TOENAME VAN RANSOMWARE

ONVOLDOENDE BESCHERMING

EIGEN BEHEER VAN CYBERSECURITY

ARTIFICIAL INTELLIGENCE: EEN TWEESNIJDEND ZWAARD IN CYBERSECURITY



In een wereld waar technologie zich in een razendsnel tempo ontwikkelt, is cybersecurity een belangrijke zorg geworden voor bedrijven over de hele wereld, en ook voor die van u! Met de opkomst van artificial intelligence (AI) neemt deze zorg een nieuwe dimensie aan, waarbij de uitdagingen rond de bescherming van gegevens en systemen steeds complexer worden.

De toenemende integratie van artificial intelligence in ons leven biedt onmiskenbare voordelen, maar brengt ook aanzienlijke risico's met zich mee. Zoals Sam Altman, CEO van OpenAI, uitgever van ChatGPT, benadrukte, vertegenwoordigt AI potentieel het eerste gevaar van deze technologie. In feite kunnen AI-algoritmen, naarmate ze geavanceerder worden, ook kwaadaardig worden ingezet om grootschalige cyberaanvallen te plegen.

In deze context is de jaarlijkse cybersecuritybarometer van Skyforce een essentieel hulpmiddel om de trends, uitdagingen en opkomende oplossingen in de wereld van de informatiebeveiliging te begrijpen. Bij Skyforce nemen we de implicaties van artificial intelligence op cybersecurity zeer serieus, evenals de strategieën en technologieën die nodig zijn om deze nieuwe realiteit het hoofd te bieden.

Wij nodigen u uit om in dit rapport te duiken, het resultaat van diepgaande analyse en gespecialiseerde expertise, om de cruciale kwesties die de toekomst van cybersecurity vormgeven beter te begrijpen.

Dominique Mangiatordi

Co-Founder & AI Expert

SKYFORCE CYBER SECURITY

1. PROFIELEN-TYPE

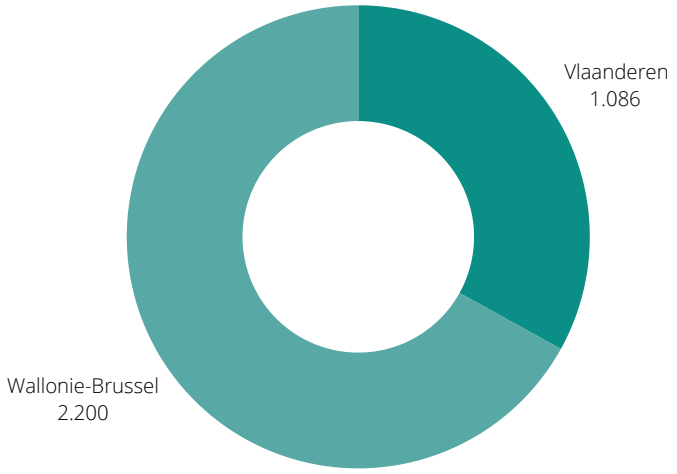
Bevraagde bedrijven

Typische profielen van deelnemende bedrijven

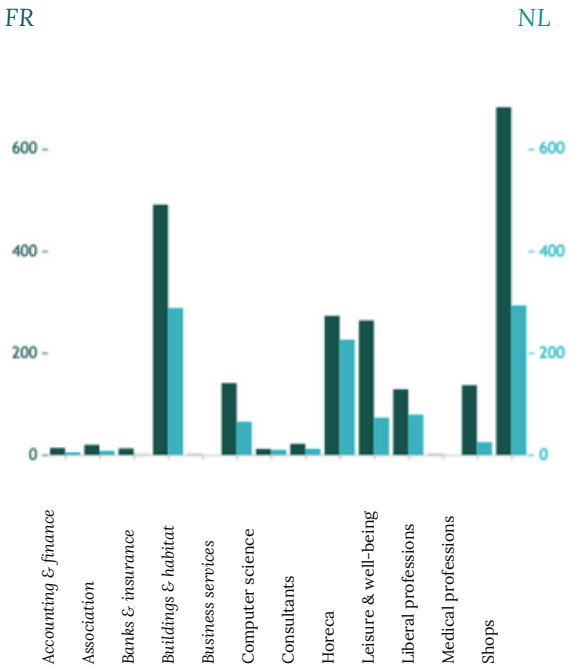
Onze consultants hebben heel België doorkruist, van grote stedelijke gebieden tot de meest afgelegen gemeenten en dorpen. In bijna alle gevallen was onze gesprekspartner de algemeen directeur of medewerker van het bedrijf.

De steekproef is niet alleen zeer groot, maar ook zeer gevarieerd qua bedrijfssectoren: handel (in brede zin), bouw en huisvesting vormen de meest vertegenwoordigde werkterreinen (samen 53% van de ondervraagden). Dit zijn ook de sectoren die het weefsel vormen van kleine ondernemingen in België.

GEÏNTERVIEWDE BEDRIJVEN



ACTIVITEITENGEBIED



FOCUS OP KMO'S

Aantal werknemers

1 werknemer	28,52%
Tussen 2 en 5	60,50%
Meer dan 5	10,98%

Het onderzoek richtte zich op zeer kleine bedrijven, zoals blijkt uit het feit dat 89,02% van de 3.286 geïnterviewde bedrijven minder dan 5 medewerkers in dienst heeft. Hoewel 10,98% van de ondervraagden afkomstig is van bedrijven met meer dan 5 medewerkers, behoort slechts 3,73% tot bedrijven met meer dan 10 medewerkers.

SKYFORCE CYBER SECURITY

2. GEBRUIK VAN EN AANWEZIGHEID OP

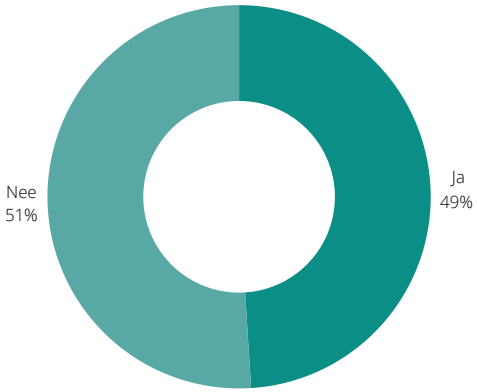
Het Internet

Gebruik en aanwezigheid op het internet

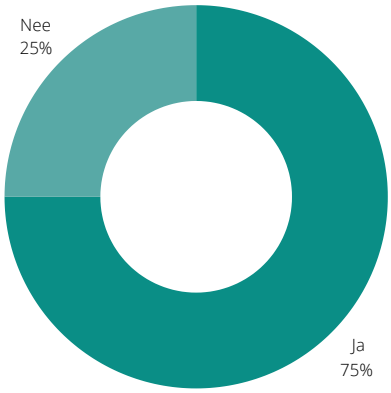
Heeft u een website?

Nederlandstalige ondernemers lijken nog steeds meer geneigd te zijn dan Franstalige ondernemers om een website te hebben, met 75% van hen die een eigen website hebben in vergelijking met 49% aan de Waalse kant.
Over het algemeen heeft 58% van de leidinggevenden een website.

FR



NL

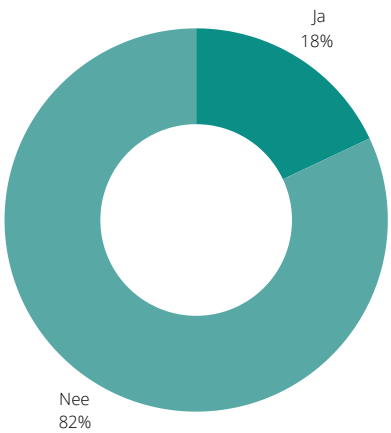


Heeft u een webshop?

Net als vorig jaar blijft 88% van de ondervraagde leidinggevenden zonder e-commerce website, ondanks het succes van online aankopen. In feite hebben Belgen bijna 8 miljard euro online uitgegeven in de eerste helft van 2023.

FR

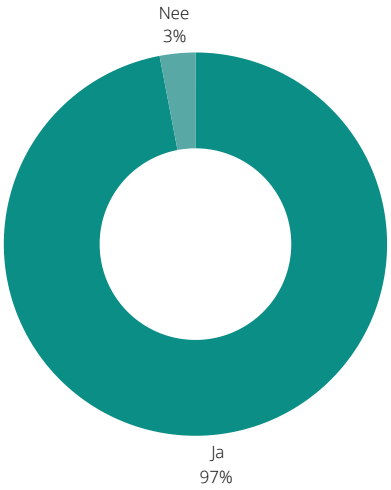
NL



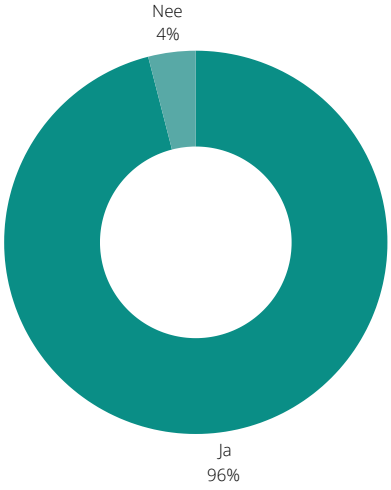
Online bankieren en online winkelen

Doet u uw bankzaken en/of aankopen via internet?

FR



NL



97% van de managers blijven hun bankzaken online regelen, en dit percentage is onveranderd ten opzichte van het voorgaande jaar.

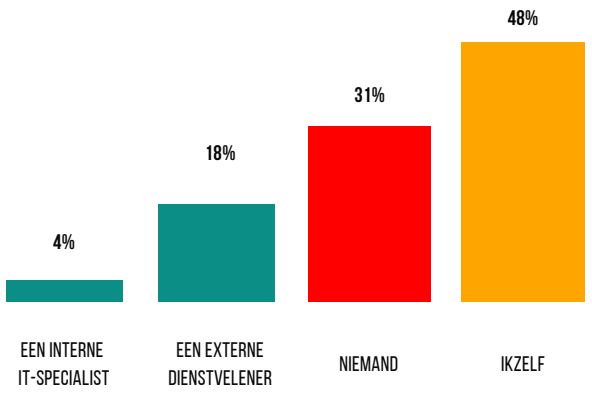
3. BESCHERMING

Stand van zaken

Beveiliging van onze KMO'S

Slechts 22% van de bedrijven doet een beroep op een professional, zoals een IT-specialist of een externe dienstverlener, om hun IT-beveiliging te waarborgen. In 78% van de gevallen wordt deze taak uitgevoerd door de directeur of door niemand.

Wie beheert de IT-beveiliging in uw bedrijf?



Deze constatering is des te zorgwekkender omdat steeds meer ondernemers hun cyberbeveiliging zelf beheren.
Het is cruciaal dat bedrijfsleiders de noodzaak van professionele IT-beveiliging inzien. Deze passage benadrukt de dringende noodzaak voor bedrijfsleiders om actie te ondernemen in het licht van een afname van bepaalde beveiligingspraktijken, en onderstreept het vitale belang van cyberbeveiliging in de huidige context.

KLEINE BEDRIJVEN, MEER BLOOTGESTELD AAN CYBERAANVALLEN

Bewust van het feit dat ze vaak beperkte middelen en verdedigingsmogelijkheden hebben, richten hackers zich specifiek op kleine bedrijven.

De gevolgen van een cyberaanval kunnen echter verwoestend zijn, variërend van aanzienlijke financiële verliezen tot schade aan de reputatie en verlies van klanten.

Het is daarom essentieel dat deze kleine bedrijven proactieve maatregelen nemen om hun beveiliging te versterken.

Bescherming, stand van zaken

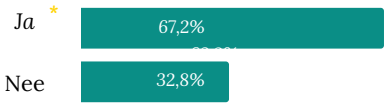
Jaar na jaar onthullen onze audits een constante trend: de meerderheid van de bedrijven implementeert geen volledige bescherming tegen online bedreigingen.

Dit jaar is de gegevensversleuteling opmerkelijk verbeterd. Gewoonlijk genegeerd door bedrijfsleiders, is deze met **44,44%** toegenomen, wat wijst op een groeiend bewustzijn van het belang ervan voor de bescherming van vertrouwelijke en gevoelige informatie.

Daarentegen is het gebruik van een firewall en het maken van back-ups van gegevens aanzienlijk afgenomen, ondanks hun goede vooruitgang in de voorgaande jaren. Het gebruik van een firewall is met **16,26%** gedaald, wat wijst op een terugval in de bescherming van netwerken tegen externe bedreigingen. Bovendien zijn regelmatige gegevensback-ups, hoewel essentieel voor de continuïteit van een bedrijf, met **29,88%** afgenomen, wat bijzonder zorgwekkend is op het gebied van cybersecurity. In geval van een cyberaanval, zoals een ransomware-aanval of een datalek, lopen bedrijven het risico om al hun gegevens of een aanzienlijk deel ervan te verliezen als ze niet beschikken over voldoende back-ups.

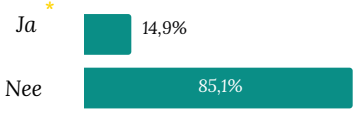
Het is om deze redenen dat wij ons inzetten om onze missie voort te zetten door geavanceerde beveiligingsoplossingen te bieden om zelfstandigen in België te ondersteunen en te beschermen.

Heeft u een antivirus?



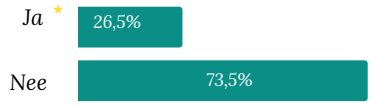
*64,5% in 2022

Heeft u een anti-spyware?



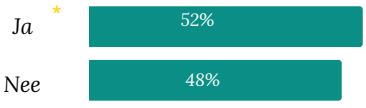
*15,9% in 2022

Heeft u een anti-spam software?



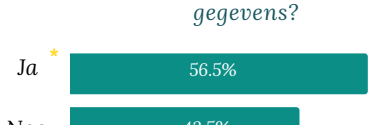
*24,9% in 2022

Heeft u een firewall?



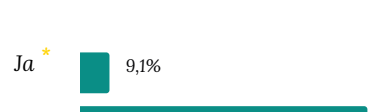
*62,1% in 2022

Maakt u regelmatig een back-up van uw gegevens?



*59,5% in 2022

Zijn uw gegevens versleuteld?



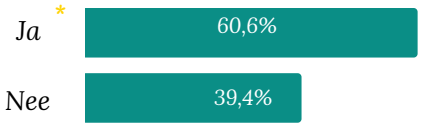
*6,3% in 2022

Verwarring privé/professioneel

De grens tussen privé- en professioneel leven is van essentieel belang, en bedrijfsleiders lijken zich daarvan bewust te worden. Dit jaar zijn er minder mensen (**-2,4%**) die het wachtwoord van hun bedrijfswifi hebben gedeeld met een externe persoon, en er zijn meer mensen (**+4,3%**) die de gegevens van hun oude apparaten hebben gewist.

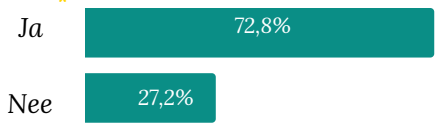
Deze ontwikkeling markeert een positieve trend naar een betere scheiding tussen privé- en professioneel leven.

Deelt u al eens uw wifi-wachtwoord met andere ?



63% in 2022

Verwijdert u gegevens van oude apparaten die u vervangt?

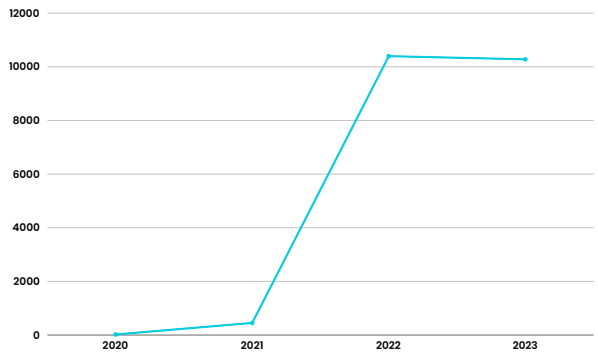


*68,5% in 2022

Enkele cijfers

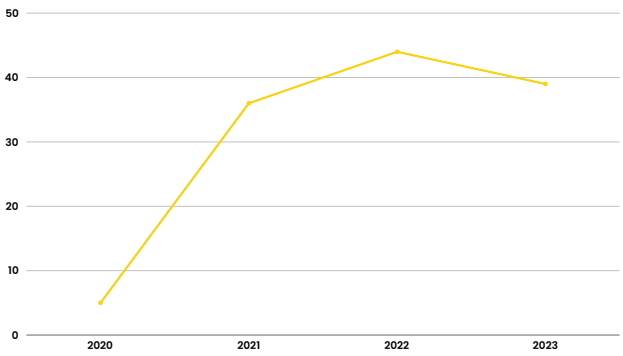
van de 3.700 zelfstandigen die beschermd worden door de Cyberbox

Phishing



Per Cyberbox / jaar

Ransomware



Per Cyberbox / jaar

De grafieken hierboven tonen het aantal **phishing- en ransomware-aanvallen** dat jaarlijks door de Cyberbox is gestopt.

De evolutie van phishing- en ransomware-pogingen vertoont een significante toename tussen 2020 en 2022, gevolgd door een lichte daling in 2023. Dit suggereert dat cybercriminelen hun inspanningen hebben opgevoerd als gevolg van de overgang naar **thuiswerken** op afstand na de **Coronavirus**-pandemie, maar ook dat ze zich steeds meer op bedrijven van alle groottes richten. De lichte daling in 2023 geeft aan dat de getroffen beschermingsmaatregelen effectiever worden. Desalniettemin blijft het hoge aantal phishingaanvragen zorgwekkend en benadrukt het de noodzaak voor kleine bedrijven om waakzaam en goed **beschermd** te blijven.

Deze cijfers illustreren duidelijk de **escalatie van cyberdreigingen** waarmee kleine bedrijven worden geconfronteerd, en benadrukken het belang van cybersecurity in het huidige digitale landschap. Bescherming tegen deze risico's vereist voortdurende **waakzaamheid**, het aannemen van geavanceerde beveiligingstechnologieën zoals Cyberbox, en een groter **bewustzijn** van goede cybersecuritypraktijken.

Met dit in gedachten blijven we de evolutie van deze aanvallen nauwlettend volgen en bieden we middelen en advies om kleine bedrijven te helpen zich te beschermen tegen deze groeiende dreigingen.

Hit-parade 2024

Het jaar 2023 heeft onze klanten niet gespaard, die te maken hebben gehad met **tienduizenden pogingen tot cyberaanvallen.** Om hun veiligheid te waarborgen, hebben we deze infecties gecorrigeerd en hieronder vindt u de rangschikking:

1. JS/ADWARE.ADPORT.A

   Applicatie.
   JS/ADWARE.ADPORT.A is een ongewenste advertentiesoftware (adware), meestal zonder medeweten van de gebruiker geïnstalleerd, vaak verborgen in gratis software die van het internet is gedownload.

2. WIN64/ROOTKIT.AGENT.AZ

   Applicatie.
   WIN64/ROOTKIT.AGENT.AZ is een kwaadaardige software die zich in uw systeem verbergt om de activiteiten van andere kwaadaardige software te camoufleren.

3. HEUR:TROJAN.SCRIPT.GENERIC

   Trojan.
   HEUR.TROJAN.SCRIPT.GENERIC identificeert verdachte scripts die vergelijkbaar zijn met Trojaanse paarden, door een analyse van hun gedrag.

4. JS/ADWARE.SCULINST.S

   Applicatie.
   JS/ADWARE.SCUNLIST.S is een adware die zich zonder toestemming installeert, opdringerige advertenties toont en informatie verzamelt over uw surfgedrag.

5. HEUR: ADWARE.SCRIPT.PUSHER.GEN

   Applicatie.

6. WIN32/YTDDOWNLOADER.H

   Applicatie.
   WIN32/YTDDOWNLOADER.H is een ongewenst programma dat vaak zonder toestemming wordt geïnstalleerd en uw computer vertraagt. Hoewel het mogelijk maakt om video's te downloaden van bekende platforms, gaat het vaak gepaard met ongewenste software.

7. HEUR: ADWARE.SCRIPT.GENERIC

   Applicatie.

8. JS/ADWARE.SCUNLIST.J

   Applicatie.

9. HTML/PHISHING.GEN

   Trojan.

10. JS/ADWARE.AGENT.CZ

    Applicatie.

Conclusie

Waarom uw bedrijf beschermen?

Regelgevende naleving

Bedrijven worden onderworpen aan wetten en regelgevingen, waaronder de Algemene Verordening Gegevensbescherming. Het is dus belangrijk om te voldoen aan de wetten en regelgevingen met betrekking tot cyberbeveiliging om deze gevolgen te voorkomen.

Financiën

Bij een cyberaanval kunnen bedrijven grote financiële verliezen lijden, onderbrekingen van de dienstverlening, kosten voor gegevensherstel.... Bovendien kunnen deze verliezen de mogelijkheid van het bedrijf om diensten of producten aan haar klanten te leveren negatief beïnvloeden, wat ook kan leiden tot een daling van de inkomsten en verlies van marktaandeel.

Reputatie

Als een essentieel onderdeel van een bedrijf kan de reputatie aanzienlijk worden beïnvloed door cyberaanvallen. Klanten kunnen het vertrouwen in het bedrijf verliezen als hun persoonlijke gegevens gestolen of aangetast zijn, wat kan leiden tot een daling van de verkoop en verlies van klanten. Bovendien kunnen de media en andere bedrijven negatieve verhalen publiceren over het bedrijf, wat ook de reputatie en het imago kan schaden.

Als Financieel Directeur van SKYFORCE Cyber Security SRL, wil ik benadrukken dat cybersecurity niet alleen een cruciaal onderdeel is van ons serviceaanbod, maar ook een essentiële component van onze eigen bedrijfsstrategie. Recente observaties op het veld en studies tonen duidelijk aan dat cyberaanvallen verwoestende gevolgen kunnen hebben voor zowel de reputatie als de financiën van een bedrijf, met een bijzondere nadruk op het belang van het beschermen van de persoonlijke gegevens van onze klanten, een verantwoordelijkheid die versterkt wordt door de GDPR.

Gezien deze uitdagingen blijft ons bedrijf proactief investeren in geavanceerde technologieën, in het versterken van de vaardigheden van onze werknemers, en in het ontwikkelen van strategische partnerschappen om ons veiligheidsecosysteem te verrijken. Dankzij onze proactieve aanpak en onze toewijding aan uitmuntendheid op het gebied van cybersecurity, streven we ernaar deze risico's te minimaliseren, onze reputatie te beschermen en een duurzame groei op lange termijn voor ons bedrijf en onze aandeelhouders te waarborgen. Door onze onderneming te beschermen tegen cyberaanvallen, beschermen we niet alleen onze financiële activa en onze reputatie, maar versterken we ook het vertrouwen van onze klanten en partners in ons vermogen om veilige diensten en producten te leveren.

Pierre-Olivier Glachant

Co-Founder & Financial Director

OVER SKYFORCE

Skyforce werd opgericht in 2019 en is gevestigd in Waterloo. Het bedrijf positioneert zich als pionier op de markt voor geïntegreerde cyberbeveiligingsdiensten voor zeer kleine, kleine en middelgrote ondernemingen.

Onze expertise is gericht op alle bedrijfssectoren. Meer dan 3.700 bedrijven in België hebben ons reeds hun cyberbeveiliging toevertrouwd, wat van Skyforce een belangrijke speler maakt op het gebied van IT-beveiliging voor kleine ondernemingen.

MISSIE

Het is onze missie om de gegevens van kleine en middelgrote ondernemingen te beschermen tegen cyberaanvallen. We ondersteunen onze klanten bij het beveiligingsbeheer van hun IT-infrastructuur, of het nu gaat om een individuele gebruiker of een netwerk.

VISIE

Innovatie, constante monitoring, de manier waarop en de zorgvuldigheid staan centraal in onze ambitie om internationaal toonaangevend te worden op het gebied van digitale beveiliging.