



CYBERBEVEILIGING - BELGISCHE MICRO-ONDERNEMINGEN EN KMO'S

JAARLIJKSE BAROMETER

2023

SKYFORCE
CYBER SECURITY



METHODOLOGIE

Jaarlijkse barometer 2023

Deze vierde Skyforce-barometer is gebaseerd op bezoeken en individuele interviews met 3.840 Belgische bedrijven, die gedurende het hele jaar 2022 zijn uitgevoerd.

Onze consultants hebben rechtstreeks de managers geïnterviewd 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 & Sales Manager

"We hechten er belang aan om onze vertegenwoordigers voortdurend op te leiden om kwaliteitsaudits te waarborgen, die consistent en grondig worden uitgevoerd. Op deze manier kunnen we ook de kwaliteit van onze diensten verbeteren"

3840 BEDRIJVEN GEPEILD

BELANGRIJKSTE PUNTEN 2023



CYBERBEVEILIGING NIET BEHEERD
DOOR EEN PROFESSIONAL



GEGEVENS NOG STEEDS NIET
VERSLEUTELD.



ONVOLLEDIGE BESCHERMING.



PHISHING WORDT STEEDS
GEAVANCEERDER.



PHISHING: BELANGRIJKE BEDREIGING.

In 2023 blijft phishing een veelvoorkomende en effectieve aanval

De methode die door cybercriminelen wordt gebruikt om vertrouwelijke gegevens zoals wachtwoorden, creditcardnummers en meer te stelen, phishing, blijft een veelvoorkomende en succesvolle aanval!

Trends in 2023:

- IA

Hackers gebruiken nu kunstmatige intelligentie-tools om geavanceerde phishing-aanvallen uit te voeren. Deze tools stellen hen in staat om automatisch frauduleuze e-mails, nepwebsites en zelfs aangepaste spraakberichten te genereren om hun doelwit te misleiden.

- Business email compromise (BEC) & email account compromise (EAC)

Dit soort technieken heeft tot doel de slachtoffers te laten denken dat ze een e-mail ontvangen van een hogere leidinggevende, om hen zo te bewegen geld over te maken of vertrouwelijke informatie te verstrekken.

- Whaling phishing

Er worden ook gerichte aanvallen uitgevoerd op hoge leidinggevenden van een bedrijf, waarbij de aanvallers zich bijvoorbeeld voordoen als zakelijke partners om gevoelige informatie of privileges te verkrijgen. Dit staat bekend als spear-phishing.



Philippe Verwerft

Co-Founder & ICT Director

"Elke dag worden we geconfronteerd met de aanhoudende en geloofwaardige phishing-aanvallen. We ontvangen regelmatig verzoeken van mensen die met dit soort aanvallen te maken hebben. We treden onmiddellijk op om deze situaties op te lossen."



1. PROFIELLEN-TYPE

Bevraagde bedrijven

Typische profielen van deelnemende bedrijven

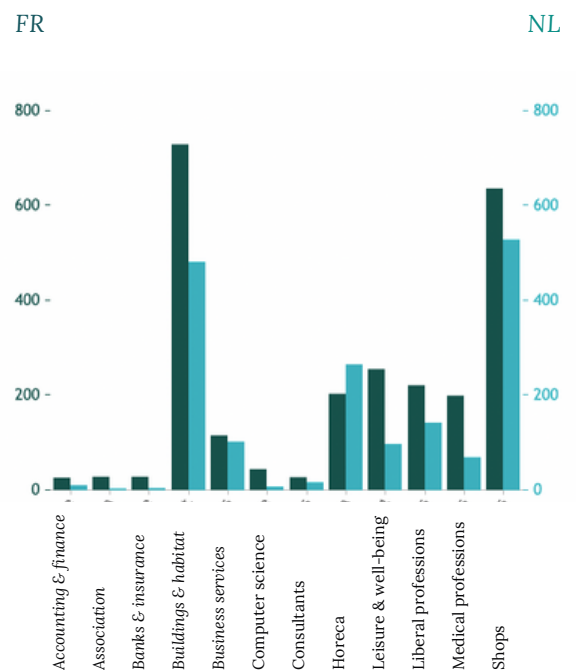
Onze consultants hebben heel België doorkruist, van grote stedelijke gebieden tot de meest afgelegen gemeenten en dorpen. In bijna alle gevallen was onze gesprekspartner de algemeen directeur of medewerker van het bedrijf.

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 62% 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	30,42%
Tussen 2 en 5	58,07%
Meer dan 5	11,51%

Het onderzoek richtte zich op zeer kleine bedrijven, zoals blijkt uit het feit dat 88,49% van de 3840 geïnterviewde bedrijven minder dan 5 medewerkers in dienst heeft. Hoewel 11,51% van de ondervraagden afkomstig is van bedrijven met meer dan 5 medewerkers, behoort slechts 3,86% tot bedrijven met meer dan 10 medewerkers.



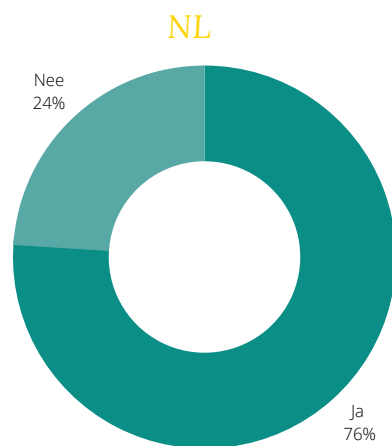
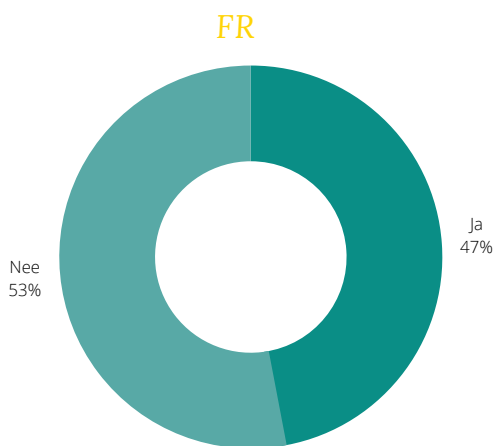
2. GEBRUIK VAN EN AANWEZIGHEID OP

Het Internet

Gebruik en aanwezigheid op het internet

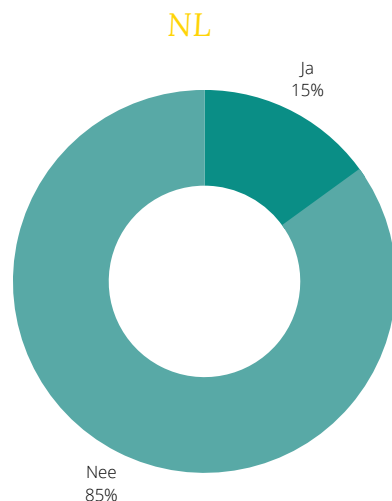
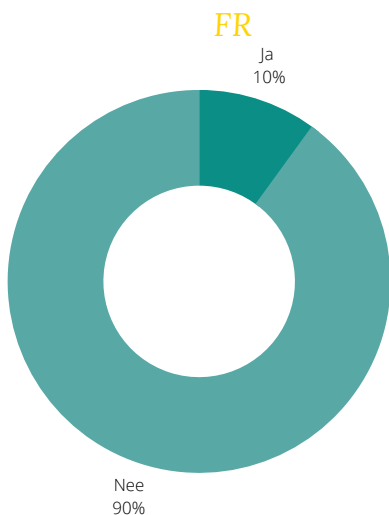
Heeft u een website?

De situatie blijft hetzelfde in vergelijking met voorgaande jaren. De geïnterviewde managers hebben nog steeds zeer verschillende internetgebruiken. Er is een duidelijk regionaal onderscheid, maar wereldwijd beschikt 62% van de respondenten over een website.



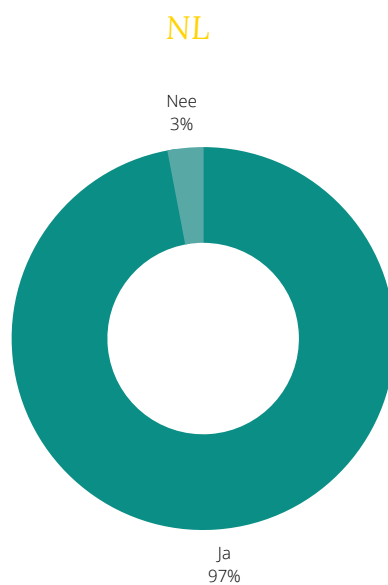
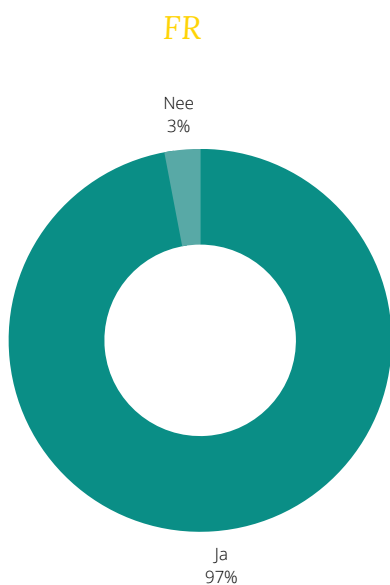
Heeft u een webshop?

De situatie blijft stabiel: in totaal heeft 88% van de respondenten geen e-commerce website, wat vergelijkbaar is met voorgaande jaren. Hoewel online verkoop is toegenomen door digitalisering en de gezondheids crisis, hebben de respondenten nog steeds weinig e-commerce websites, ondanks de moeilijkheden om hun publiek online te bereiken.



Online bankieren en online winkelen

Doet u uw bankzaken en/of aankopen via internet?



97% van de managers blijft hun bankzaken online regelen, en deze verhouding blijft stabiel ten opzichte van vorig jaar, met een toename van slechts 1%.

97%

MANAGERS DOEN HUN
BANKZAKEN VIA INTERNET





3. BESCHERMING

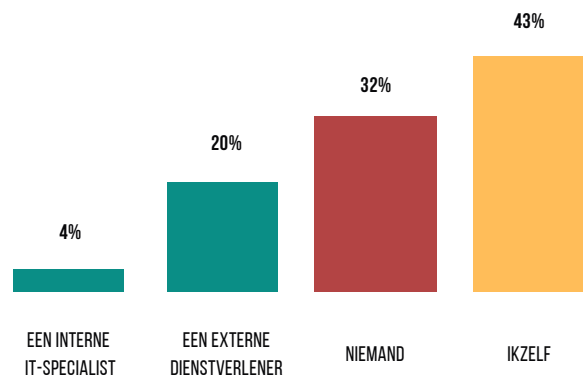
Stand van zaken

Beveiliging van onze KMO'S

Slechts 24% van de bedrijven doet een beroep op een professional, zoals een IT-specialist of een externe dienstverlener, om hun IT-beveiliging te waarborgen. In 76% van de gevallen wordt deze taak uitgevoerd door de directeur of door niemand.

Ondanks een lichte stijging van 4% van de ondernemers die kiezen voor professionele computerbeveiliging, blijft de situatie zorgwekkend. Bijna alle cyberaanvallen kunnen echter eenvoudig worden voorkomen.

Wie beheert de IT-beveiliging in uw bedrijf?



KLEINE BEDRIJVEN ZIJN HET VOORNAAMSTE DOELWIT VAN CYBERAANVALLEN.

Hackers zijn nog steeds op zoek naar gemakkelijke doelwitten en helaas staan kleine bedrijven vaak bovenaan hun lijst. Ze weten dat kleine bedrijven vaak minder middelen en minder tijd hebben om zich te beschermen tegen cyberaanvallen en daardoor kwetsbaarder zijn voor hun aanvallen.

Daarom is het essentieel dat kleine bedrijven online beveiligingsmaatregelen nemen om zichzelf te beschermen tegen deze hackers.

Bescherming, stand van zaken

De eerste observatie is dat de meerderheid van de ondervraagde bedrijven in het beste geval een onvolledige bescherming hebben, ondanks hun steeds grotere digitale blootstelling en de steeds bekwaamere hackers.

Er is echter een toename in het gebruik van een firewall (+19,65%), anti-spam software (+22,06%), en de voortdurende vooruitgang in back-up gebruik (+5,7%). Bewustwording lijkt dus nog steeds door te dringen bij de bedrijfsleiders die zich niet langer afvragen of ze ooit het doelwit van een aanval zullen zijn, maar eerder wanneer en hoe dit zal gebeuren.

Niettemin loopt bijna de helft van de ondervraagde bedrijven nog steeds het risico om hun gegevens te verliezen bij een cyberaanval.

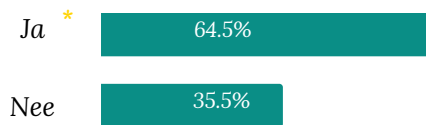
Bovendien blijft encryptie van gegevens en apparaten verwaarloosd in kleine bedrijven (-23%). Dit is des te zorgwekkender omdat in het geval van inbraak de cybercrimineel gemakkelijk toegang kan krijgen tot privé-, vertrouwelijke en gevoelige gegevens, evenals wachtwoorden.

Tijdsdruk blijft een obstakel voor deze leiders die op alle fronten actief zijn om hun bedrijf te beheren.

Daarom zijn we vastbesloten om een complete oplossing en lokale service te bieden om kleine bedrijven te helpen hun bedrijfsactiviteiten te beschermen tegen deze bedreigingen.



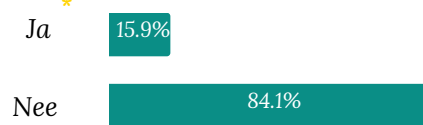
Heeft u een anti-virus?



*63.2% in 2021



Heeft u een anti-spyware?



*17.2% in 2021



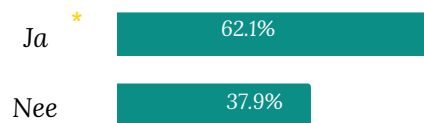
Heeft u een anti-spam software?



*20.4% in 2021



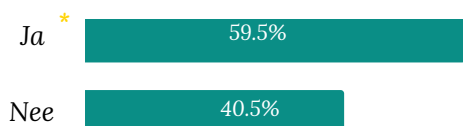
Heeft u een firewall?



*51.9% in 2021



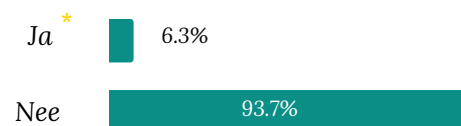
Maakt u regelmatig een back-up van uw gegevens?



*56.3% in 2021



Zijn uw gegevens versleuteld?



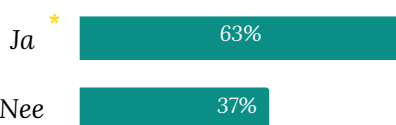
*8.2% in 2021

Verwarring privé/professioneel

De grens tussen het persoonlijke en professionele leven blijft een bron van zorg, zoals blijkt uit de statistieken: **63%** van de ondervraagden heeft het **wifi-wachtwoord** van hun bedrijf al **gedeeld** met een externe persoon. Dit is een stijging van 4% ten opzichte van 2021. Het is echter cruciaal om duidelijke **grenzen** te stellen tussen deze twee sferen, aangezien hun vermenging bijna een open uitnodiging kan zijn voor hackers en diefstal van gevoelige gegevens.

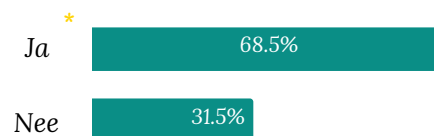


Deelt u al eens uw wifi-wachtwoord met andere ?



*59.1% in 2021

Verwijdert u gegevens van oude apparaten die u vervangt?

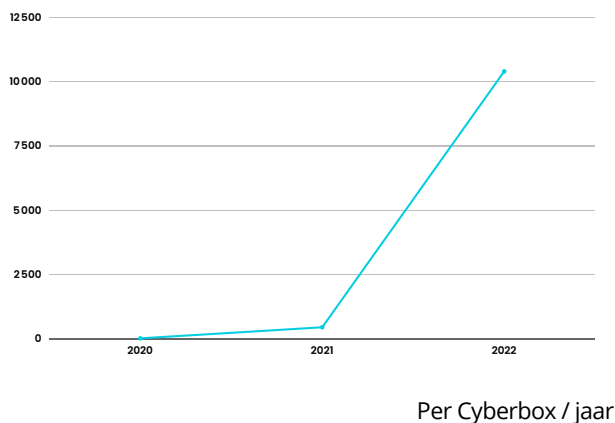


*67.7% in 2021

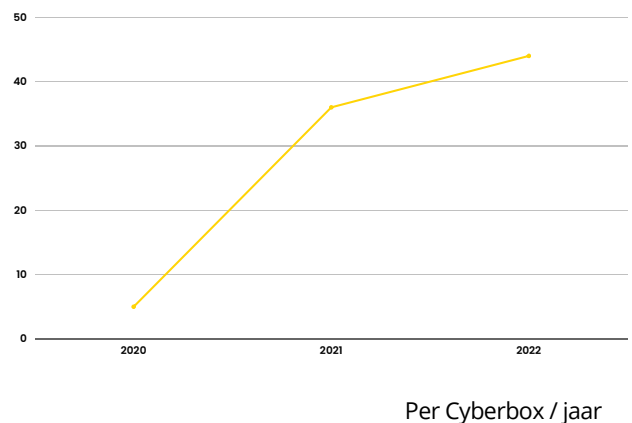
Enkele cijfers

van de 3.000 zelfstandigen die beschermd worden door de Cyberbox

■ Phishing



■ Ransomware



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

De cijfers laten duidelijk een **stijgende trend** zien in deze aanvallen.

We kunnen zien dat het gemiddelde aantal geblokkeerde ransomware-aanvallen door de Cyberbox geleidelijk is gestegen, van 5 in 2020 naar 36 in 2021 en vervolgens naar 44 in 2022, ongeveer 8 keer meer.

Voor phishing-aanvallen is de groei echter aanzienlijk groter, van 21 in 2020 naar 452 in 2021 en vervolgens naar 10.397 in 2022, bijna **500 keer hoger** in 3 jaar!

Het aantal cyberaanvallen blijft elk jaar toenemen, met steeds ernstigere **gevolgen** voor kleine bedrijven. Met oog voor het belang van cyberbeveiliging blijven we de ontwikkeling van cyberaanvallen nauwlettend volgen en **hulpbronnen** en **advies** bieden om kleine bedrijven te helpen zich te beschermen tegen deze toenemende dreigingen.

Hit-parade 2022

Het jaar 2022 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. HEUR:TROJAN.SCRIPT.GENERIC

Trojan

2. JS/ADWARE.ADPOR.T.A

Applicatie

3. HTML/PHISHING.GEN

Trojan

4. JS/ADWARE.SCULINST.J

Applicatie

5. MSIL/AGENT.CQF

Trojan

6. JS/ADWARE.SCULINST.S

Applicatie

7. JS/ADWARE.TERRACLICKS.A

Applicatie

8. JS/ADWARE.AGENT.AY

Applicatie

9. WIN32/YTDDOWNLOADER.H

Applicatie

10. JS/PACKED.AGENT.K

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 merkimago kan schaden.



Christophe Henri

Co-Founder & Technical Operations
Manager

"Door de jaren heen heeft technologie de manier waarop we werken en met elkaar omgaan veranderd. Terwijl we profiteren van de voordelen van deze transformatie, moeten we ons ook bewust zijn van de dreigingen die ermee gepaard gaan. Cyberaanvallen worden steeds frequenter en geavanceerder, en geen enkel bedrijf is veilig. Daarom is het essentieel dat kleine bedrijven maatregelen nemen om hun gegevens en IT-infrastructuur te beschermen. Uiteindelijk is cyberbeveiliging een essentieel onderdeel van elk modern bedrijf, ongeacht de grootte. Door uw gegevens te beschermen en de beveiliging van uw IT-infrastructuur te waarborgen, kunt u uw bedrijf beschermen tegen financiële verliezen, reputatieschade en andere rampzalige gevolgen van cyberaanvallen."

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 3.200 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 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.

