Cyber Challenge

UW ONDERNEMING BESCHERMEN IN HET DIGITALE TIJDPERK : uitdagingen en *best practices*

CYBERSCAN
economie
nsz neutraal syndicaat voor zelfstandigen
Gefinancierd door de Europese Unie
NextGenerationEU

Webinars *Cyber Challenge*

In het raam van het project Cyber Challenge werden diverse webinars georganiseerd om zelfstandigen, kmo's en vrije beroepen bewust te maken van de belangrijkste uitdagingen op het vlak van cybersecurity.

Tijdens deze onlinesessies kwamen de risico's aan bod waar bedrijven vandaag het vaakst mee te maken krijgen (phishing, accounthacking, dataverlies, enz.). Daarnaast werden praktische en laagdrempelige tips meegegeven om de business in de dagelijkse praktijk beter te beveiligen.

De webinars behandelen onder meer:

- de meest voorkomende cyberdreigingen voor kleine organisaties;
- *best practices* op het vlak van digitale veiligheid;
- eenvoudige tools en maatregelen om gegevens beter te beschermen;
- begeleidende oplossingen die in het raam van het project Cyber Challenge worden aangeboden.

U kunt de webinars opnieuw bekijken via onderstaande links:

- Cybersecurity voor zelfstandigen en kmo's: https://youtu.be/K2UuHb7ff84
- Cybersecurity voor handelaars: https://youtu.be/LaVLT5NnkIM

Lees in *De Zelfstandige* over wat u en ons bezighoudt

NSZ publiceert elke maand *De Zelfstandige*, een tijdschrift gewijd aan de informatie en de ondersteuning van zelfstandigen en kmo's in België. In de diverse rubrieken van het tijdschrift zoomen wij in op de economische, politieke en regelgevende uitdagingen die een rechtstreekse impact hebben op de business van ondernemers.

In elk nummer vindt u analyses, thematische dossiers en diepgravende artikels over onderwerpen die voor zelfstandigen van cruciaal belang zijn: de evolutie van de wetgeving, de sociaaleconomische actualiteit, de digitalisering van ondernemingen, cybersecurity, artificiële intelligentie, bedrijfsvoering of nog de transformatie van handel en beroepen. Bedoeling: ondernemers heldere en concrete informatie verstrekken waar ze in hun dagelijkse professionele realiteit meteen iets mee kunnen.

Voorts vindt u in ons tijdschrift praktische tips, didactische fiches, vragen en antwoorden rond juridische kwesties en getuigenissen van ondernemers en experten. Stuk voor stuk bijdragen die best practices toelichten, vertellen over ervaringen van échte mensen in het veld en zorgen dat zelfstandigen beter voorbereid zijn op de uitdagingen die ze op hun pad vinden.

Via De Zelfstandige informeert, sensibiliseert en begeleidt NSZ ondernemers, zodat zij hun business bestendig kunnen uitbouwen en beveiligen.

Alle NSZ-leden hebben gratis toegang tot het tijdschrift.

Meer weten over de diensten van NSZ en de aansluitingsvoorwaarden? Neem een kijkje op www.nsz.be

VOORWOORD DOOR ALGEMEEN DIRECTEUR

Zelfstandigen beschermen tegen cyberdreiging: wij gaan er 100% voor!

Cybersecurity is vandaag een strategische uitdaging voor zelfstandigen en kmo's. Naarmate de digitalisering – denk maar aan cloudtoepassingen, artificiële intelligentie, sociale media, elektronische facturering en e-commerce — versnelt, nemen de groeikansen toe. Maar tegelijk ook de risico's.

Het project *Cyber Challenge* kadert in die realiteit. Het past ook binnen de bredere Europese dynamiek om de digitale weerbaarheid te versterken, een dynamiek die wordt gesteund door het Europese relanceplan *NextGenerationEU*, onder meer via initiatieven zoals *Cyber4SME*, uitgerold door de FOD Economie. De doelstelling is duidelijk: zelfstandigen en kmo's concreet begeleiden in een klimaat van toenemende cyberdreiging en hen voorbereiden op de vereisten van de nieuwe Europese regelgeving.

NSZ wil met dit project een toegankelijke, pragmatische en praktijkgerichte aanpak bieden. Het is niet de bedoeling het dagelijkse beheer nog ingewikkelder te maken voor ondernemers, wel hen in staat te stellen prioriteiten te bepalen, hun werkwijze te versterken en hun business op proportionele wijze te beveiligen.

Dit witboek vat de bevindingen, inzichten en *best practices* samen die zijn voortgevloeid uit *Cyber Challenge*. Het toont aan dat doeltreffende cybersecurity in de eerste plaats gestoeld is op eenvoudige, gestructureerde maatregelen die zijn afgestemd op elke professionele realiteit.

Wie zijn digitale veiligheid versterkt, beschermt zijn onderneming, zijn klanten en de continuïteit van zijn business. NSZ zal zich blijven inzetten om de weerbaarheid van zelfstandigen standvastig te ondersteunen.

Philippe Ruelens
Algemeen directeur van het Neutraal Syndicaat voor Zelfstandigen

Inhoudsopgave

Éditeur responsable :
Het Neutraal Syndicaat voor Zelfstandigen

Rédacteur :

Collaborateurs :

Conception graphique : V&Com srl

Date du magazine :

De uitdagingen van cybersecurity in de komende tien jaar

Door de technologische versnelling is ook het risico op beveiligingsproblemen groter. In een wereld waarin connectiviteit de zuurstof van de economie vormt, kan cybersecurity niet meer als louter technische functie naar het achterplan worden verwezen. Cybersecurity werpt zich vanaf nu op als de strategische hoeksteen van moderne good governance. Hierna een analyse van de ingrijpende omwentelingen waar organisaties het komende decennium voor staan.

Het digitale landschap van de komende tien jaar zal niet gewoonweg een verlengstuk zijn van het huidige: het ziet ernaar uit dat er ingrijpende omwentelingen op ons afkomen en dat veiligheid een conditio sine qua non wordt voor elke standvastige business. Morgen zal het niet langer de vraag zijn of een onderneming zichzelf goed kan beschermen, maar wel hoe ze digitale veerkracht integreert in haar groeimodel. De evolutie van artificiële intelligentie vormt een eerste grote uitdaging. Al mag dan al ongeziene productiviteitswinst opleveren, ze verplicht organisaties ook hun beveiliging tegen het licht te houden en die reactiever te maken. De beveiliging van morgen zal proactief moeten zijn, d.w.z. in staat om zelfs zwakke signalen te herkennen en automatisch komaf te maken met onregelmatigheden, dit om de continuïteit van het werk te garanderen. Deze automatisering zal geen luxe zijn, maar wel een noodzaak om aanvallen af te weren die worden aangestuurd door algoritmen die in enkele seconden duizenden barstjes in de verdediging kunnen testen.

Beveilig uw gegevens overal en voor altijd

Deze evolutie gaat gepaard met een totale dataverspreiding. Nu hybride werk gemeengoed is en geconnecteerde voorwerpen alomtegenwoordig zijn, vervaagt de traditionele perimeter van de onderneming. Een ‘business beschermen’ zal over tien jaar betekenen dat elk interactiepunt – van industriële sensor tot mobiele terminal – moet worden beveiligd. Dat zal een aanpak vergen waarbij het vertrouwen bij elke stap wordt getoetst (*Zero Trust*-architectuur). Tegelijk zal de komst van nieuwe rekenmogelijkheden – denk maar aan kwantumcomputers – ons dwingen onze encryptiestandaarden geleidelijk te actualiseren, om ook op lange termijn de onschendbaarheid van bedrijfsgeheimen en van intellectuele eigendom te verzekeren. Die kentering naar postkwantumcryptografie wordt een van de meest strategische werven van het decennium, willen we vermijden dat de digitale archieven van vandaag leesbaar worden voor de processors van morgen.

De cloudafhankelijkheid zal gevolgen hebben

Ook de kwestie van digitale autonomie en digitale afhankelijkheid zal een nieuwe dimensie krijgen. Bedrijven steunen almaar meer op wereldwijde cloudinfrastructuren, met heel wat risico’s tot gevolg. Als één belangrijke leverancier in de fout gaat, kan dat duizenden kmo’s tegelijk verlammen. In het komende decennium zullen bedrijfsleiders dus verplicht zijn hun ‘digitale toeleveringsketen’ even nauwgezet onder de loep te nemen als hun fysieke logistieke stromen. Cybersecurity zal niet langer stoppen aan de muren van de organisatie, maar ook het volledige ecosysteem van partners en onderaannemers van die organisatie omvatten. Het bedrijf zal over de hele lijn aansprakelijk zijn. Er zullen dus niet enkel ketenbrede beveiligingsaudits nodig zijn, maar ook totale transparantie over de methodes voor gegevensopslag en -verwerking.

Digitale beveiliging als bewijs van uw sérieux

Ook in menselijk en strategisch opzicht wordt het een uitdagend decennium. Cybersecurity zal niet langer worden beschouwd als een technische barrière, maar wel als een pijler van good governance en als een bewijs van professionaliteit. Een prima digitale reputatie wordt het kostbaarste bezit van een merk: een onderneming die niet in staat is de gegevens van haar klanten te beschermen, zal onmiddellijk uit de markt vallen. Het regelgevende kader tekent zich almaar duidelijker af – denk maar aan de Europese NIS2-richtlijn – en dus wordt digitale maturiteit een cruciaal criterium bij het kiezen van partners. Succes zal enkel zijn weggelegd voor organisaties die beveiliging hebben weten te verheffen tot een gedeelde cultuur. Een cultuur waarin elke medewerker, goed geïnformeerd en geruggensteund door robuuste tools, bijdraagt tot de algehele stabiliteit en de continuïteit van de organisatie in een hypergeconnecteerde wereld.

Cybersecurity breekt definitief uit de informatica-context en wordt een voorwaarde om economisch te overleven. In het licht van de kwantumdreiging en geautomatiseerde aanvallen zullen bedrijven dus niet enkel moeten investeren in technologie, maar bovenal in vertrouwen en in een cultuur van waakzaamheid. Het vermogen om de eigen stromen en data te beschermen, zal niet langer een concurrentievoordeel zijn: het wordt simpelweg een must om op de markt van morgen te kunnen bestaan.

Een zelfstandige deelt zijn ervaring met de Cyber Challenge

In het kader van de Cyber Challenge stemde Kristiaan De Roeck ermee in om deel te nemen aan een digitale audit om de beveiliging van zijn online activiteiten te evalueren en te versterken. We hebben hem gevraagd om zijn ervaring met ons te delen. Hoe heeft hij het initiatief ontdekt? Wat heeft hij ervan geleerd? En vooral: wat is er concreet veranderd in zijn dagelijks leven als zelfstandige?

BV De Werkkamer –

Kristiaan De Roeck

Kunt u zichzelf voorstellen en ons iets vertellen over uw zaak?

BV De Werkkamer is een eenmanszaak, opgericht in 1999 als restauratie- en maakatelier van meubelen, schilderijen en objecten. Geleidelijk aan breidde De Werkkamer haar activiteiten uit met het uitvoeren van projecten die restauratie en renovatie combineren, zowel in privé- als in openbare context.

Hoe hebt u over de Cyber Challenge gehoord en wat heeft u gemotiveerd om deel te nemen?

Via het NSZ Magazine. Twee elementen motiveerden me om dit te doen: een onafhankelijke toets van de veiligheid en beveiliging van de IT-omgeving van De Werkkamer en een basis die kan toelaten om op een gedefinieerde manier een cyberverzekering af te sluiten. Dit laatste vind ik erg belangrijk.

Hoe zou u vóór deze audit uw online aanwezigheid beschrijven?

De Werkkamer probeert bewust de digitale aanwezigheid te richten op de combinatie van website en e-mail. Er is een beperkte aanwezigheid op sociale media, voornamelijk omdat de tijd ontbreekt om dit grondig aan te pakken en er prioriteit wordt gegeven aan de kernactiviteiten van De Werkkamer, in functie van het karakter van een eenmanszaak.

Waaruit bestond de Cyber Challenge concreet voor u?

De Cyber Challenge bestaat uit een vraaggesprek en een achterliggende evaluatie van de website. Dit resulteert in een vrij gedetailleerd rapport waarin ook praktische elementen worden aangereikt om de digitale omgeving te optimaliseren.Een deel hiervan heb ik gedeeld met de serviceprovider die de hosting verzorgt, met het oog op de activatie van bijkomende veiligheidslagen die zowel het e-mailverkeer als de website beter beschermen. Andere elementen heb ik zelf kunnen implementeren, zoals bijvoorbeeld een betere scheiding tussen het private en het zakelijke karakter van het e-mailverkeer.

Hoeveel tijd heeft dit u gekost en was dit combineerbaar met uw dagelijkse activiteit?

Het vraaggesprek en de interpretatie van de uitkomst hebben ongeveer een halve dag tijd gekost. De activiteiten om de digitale omgeving tot hiertoe te optimaliseren namen in totaal een tweetal dagen in beslag, wel gespreid in de tijd.

Vond u de aanpak toegankelijk en begrijpelijk, ook zonder specifieke technische expertise?

Zeer zeker. Wat ook belangrijk is: dit gebeurt zonder druk. De optimalisatiedomeinen worden op een duidelijke manier aangereikt, wat ook motiveert om er effectief mee aan de slag te gaan

Werd tijdens de audit aandacht besteed aan gegevensbescherming en cybersecurity? Was u reeds gesensibiliseerd rond deze thema's en heeft dit uw manier van omgaan met klantgegevens of digitale tools veranderd?

Beide elementen komen zeker aan bod en worden, zoals aangegeven, ook opgenomen in de aanbevelingen in het rapport om de IT-omgeving te verbeteren.

Wat waren de belangrijkste aanbevelingen die u zijn bijgebleven of die u hebben verrast?

De kwaliteit van het rapport is bijzonder goed.

Bent u van plan deze aanbevelingen snel in de praktijk te brengen? Zo ja, waarmee gaat u beginnen?

Alles wat door de serviceprovider en hoster van de website kon worden aangescherpt, is intussen uitgevoerd. Boven op de bestaande cyberbeveiliging op basis van ESET is er nu ook een VPN actief. Verdere actiepunten op de agenda zijn de versleuteling van bestanden, de implementatie van een back-up in de cloud en het opstellen van een procedure bij uitval van de IT-omgeving, waarin ook een inventaris wordt opgenomen van alle gerelateerde apparatuur en netwerkadressen.

Welke concrete voordelen kan uw zaak volgens u halen uit deze digitale audit?

Idealiter kijk ik naar dit type oefening als een stappenplan. Cyber Challenge biedt een eerste helikopterzicht op de veiligheidsaspecten van data- en netwerkbeveiliging, dat ver genoeg gaat om eenvoudige verbeteringen zelf uit te voeren of te laten uitvoeren. Complexere problemen worden niet uit de weg gegaan, maar vereisen een grondigere aanpak, waarbij het rapport zeker helpt om gespecialiseerde experten aan te spreken. Via Cyber Challenge zou een bijkomende dienst kunnen worden uitgewerkt en aangeboden, betalend, om een volledig actieplan op te stellen en dit professioneel te laten begeleiden. Dit brengt me tot één van mijn belangrijkste motivatoren: het auditeren en aanpassen van de IT-omgeving om een cyberverzekering op een duidelijke en onderbouwde manier af te sluiten en verder te laten evolueren. Zo kan worden vermeden dat bij een cyberaanval "kleine of niet-gelezen lettertjes" worden ingeroepen om aansprakelijkheid te verwerpen of te beperken.

De manier waarop cyberverzekeringen vandaag op het niveau van kleinere KMO's worden afgesloten, vind ik onvoldoende gebaseerd op objectieve criteria. Hier kan Cyber Challenge een belangrijke rol spelen.

BV De Werkkamer – *Kristiaan De Roeck*
www.dewerkkamer.be

Internet, VPN en AI: juiste reflexen zijn vitaal om uw data te beveiligen

De digitale transformatie van beroepswerkzaamheden biedt grote groeikansen, maar vergt ook voortdurende waakzaamheid: nu de dreiging almaar verraderlijker wordt, is bescherming van de werkomgeving een topprioriteit. Doeltreffende beveiliging steunt niet op een mirakeloplossing, wel op een totaalaanpak die robuuste software combineert met technologische hygiëne en gezond verstand. Hierbij onze tips om daar met succes werk van te maken.

Gegevensbescherming is niet iets wat u gauw in elkaar flanst. Alles begint met de keuze van de geschikte tools. Vervolgens is het zaak uw dagelijkse gewoontes daarop af te stemmen. Een robuuste digitale omgeving bouwt u uit in vier cruciale stappen.

1 Bereid uw werkomgeving voor

Uw browser is uw eerste verdedigingslinie. Zorg dat u die goed beschermt.

- **Kies een browser die de nadruk legt op veiligheid** (bv. een correct geconfigureerde *Firefox* of *Brave*): geef de voorkeur aan de opties die focussen op privacy en die bedreigingen afblokken nog vóór ze verschijnen.
- **Bouw filters in:** installeer extensies die er specifiek op gericht zijn kwaadaardige advertenties en trackers tegen te houden. Let wel: download extensies altijd via erkende platformen (bv. *Google Play Store*)! Check het aantal gebruikers, de datum van de meest recente update en de reviews.
- **De gulden regel:** klik nooit op "*later*" voor een update. Updates zijn er net om de veiligheidslekken te dichten waar cybercriminelen maar al te graag gebruik van maken.

2 Hanteer de juiste reflexen op het internet

De technologie doet veel, gezond verstand doet de rest.

- **Check of u een 'hangslotje' ziet:** vóór u uw wachtwoord intikt, controleert u steeds of de URL in de adresbalk wordt voorafgegaan door het https-protocol.
- **Blijf waakzaam:** phishing wordt almaar geraffineerder. Bij de geringste twijfel over een e-mail of een link klikt u niet!
- **Wis uw sporen:** beperk het gebruik van cookies. Kies doelgericht welke cookies u aanvaardt of weiger ze systematisch, zodat u de controle behoudt over uw persoonsgegevens.

3 VPN : een niet te onderschatten bondgenoot

VPN staat voor **Virtual Private Network. Zo'n virtueel privénetwerk** beveiligt de gegevensoverdracht. Het wijzigt uw geolocatie, maar beschermt niet tegen phishing en niet tegen virussen.

- **Het nut:** als u een openbare wifi gebruikt, beschermt een VPN u door uw eigen IP-adres te vervangen door dat van de VPN-provider.
- **Kijk uit voor misvattingen:** een VPN is nog niet alles. Als u inlogt op uw professionele account of uw Facebookaccount, weet het platform nog altijd wie u bent.
- **Vertrouwen boven alles:** Omdat al uw internetverkeer via deze provider verloopt, kiest u er het best eentje met een onberispelijke reputatie (bv. *Proton VPN*).

4 Schakel AI in zonder risico's te nemen

Artificiële intelligentie is een briljante assistent, maar kan bij verkeerd gebruik een bron worden van massale datalekken.

- **Datadiscipline:** deel nooit vertrouwelijke informatie (naam, voornaam, adres, e-mails, medische gegevens, telefoonnummer e.d.) of bedrijfsgeheimen op een openbare AI-toepassing. Eenmaal u ze hebt ingevoerd, hebt u er geen enkele controle meer over.
- **Wees op uw hoede voor 'hallucinaties':** AI kan met onthutsende stelligheid onwaarheden poneren. Het is dus cruciaal dat u de informatie die artificiële intelligentie aanlevert, verifieert.
- **U hebt het laatste woord:** beschouw AI als een razendsnelle stagiair die af en toe verstrooid is. U moet **zijn werk dus stelselmatig controleren** vóór u het goedkeurt.

Hoe herkent u een **phishingmail**?

1. Vertrouw niet blindelings op de naam van de afzender:
ga niet af op de weergegeven naam (bv. "*Microsoft Support*"). Check het e-mailadres achter die naam. Staat er bv. "*support@microsoft-security-fix.net*" in plaats van "*@microsoft.com*"? Dan moet er een alarmbel rinkelen!

2. Beweeg uw muis over een link zonder te klikken:
dit is de meest efficiënte controle. Alvorens u op een balkje of een blauwe link klikt, plaatst u uw muisaanwijzer erop (zonder te klikken!). Check welke URL er links onderaan op uw scherm verschijnt.

3. Haast en spoed is nooit goed:
hoogdringendheid is zelfs uw ergste vijand. Cybercriminelen proberen uw gezond verstand uit te schakelen door uw emoties te bespelen. Bepaalde formuleringen zijn verdacht: "*Onmiddellijke actie vereist*", "*Account geblokkeerd*", "*Onbetaalde factuur*", "*Laatste verwittiging*". Als u via een e-mail wordt verzocht om onmiddellijk iets heel belangrijks te doen, is het waarschijnlijk een fraudepoging.

Toegangs- en wachtwoordbeheer moet uw prioriteit zijn

Denk niet dat enkel 's werelds beste hackers erin slagen e-mails en socialemediaprofielen te kraken. Er zijn veel cybercriminelen die gewoonweg profiteren van de zwakke plekken in uw verdediging om uw digitale leven binnen te dringen en uw data te stelen. En de zwakke plek bij uitstek is het resultaat van iets waar we ons allemaal aan bezondigen: kiezen voor een wachtwoord dat gemakkelijk te onthouden is en... dus gemakkelijk te kraken valt. Met behulp van artificiële intelligentie duurt het vandaag geen drie minuten meer om een wachtwoord te kraken, maar slechts drie seconden. Hoe zet u hackers een hak?

Uw wachtwoord is niet zomaar een code: het is de eerste verdedigingslinie rond uw digitale identiteit. In vier stappen beveiligt u uw toegangen als een heus fort.

1 De gouden regel: een wachtwoord moet LANG en INGEWIKKELD zijn

De voornamen of de geboortedata van uw naasten? De klassieke cijferreeks "*1 2 3 4*"? Een héél slecht idee. Krachtige software kan een eenvoudige code in luttele minuten kraken.

- **Het doel:** minstens 12 tekens. Aarzel niet om na het laatste teken een spatie te zetten. Zo'n spatie wordt door menig systeem nog niet herkend.
- **Het recept:** vertrek van een spreuk, een beklijvende zin, de eerste regel van uw favoriete boek of song. Doorspek die met cijfers en speciale tekens en creëer zo een wachtwoord.
- **Het resultaat:** u hebt de kraaktijd verlengd van enkele seconden naar... eeuwen. Dit is een mathematisch feit: hoe langer uw wachtwoord, hoe meer een hacker ontmoedigd raakt.

2 GEBRUIK NIET overal hetzelfde wachtwoord

Eén enkel wachtwoord voor alles, dat is het simpelste. Klopt, maar het is gevaarlijk om al uw onlineactiviteiten te beschermen met één wachtwoord.

- **Het principe:** elke toepassing haar eigen unieke wachtwoord.
- **Het voordeel:** als één website wordt gehackt, blijven uw andere accounts (bank, e-mail, sociale media) buiten schot en beveiligd.

Hoe kunt u achterhalen of het wachtwoord van uw mailbox werd gehackt? Geef het in op **https://haveibeenpwned.com/**. In geval van hacking, zelfs al dateert de poging van maanden of weken geleden, is het stellig aan te raden AL uw wachtwoorden te wijzigen. De gestolen data doen immers de ronde onder hackers op het darkweb en andere cybercriminelen kunnen proberen om uw oude inloggegevens te gebruiken op diverse platformen.

3 Een WACHTWOORDBEHEERDER gunt uw geheugen rust

We gaan er geen doekjes om winden: niemand van ons kan 50 ingewikkelde codes onthouden. Gelukkig kunt u rekenen op een wachtwoordbeheerder (of digitale kluis). Die bewaart al uw wachtwoorden op één enkele plaats, zelf beschermd door een sterk wachtwoord dat door de wachtwoordbeheerder wordt aangemaakt.

- **De wachtwoordbeheerder is uw geheugen:** u hoeft niets meer te onthouden, behalve dan het hoofdwachtwoord van uw digitale kluis, die ook voor elk platform een sterk wachtwoord genereert als u dat wilt.
- **De wachtwoordbeheerder controleert:** hij waarschuwt u als een van uw codes te zwak is of als er een probleem mee is.
- **De wachtwoordbeheerder beschermt tegen phishing:** als u op een valse website bent beland, zal de wachtwoordbeheerder weigeren de velden in te vullen. Dat is een instantbeveiliging tegen oplichting.
- **Enkele wachtwoordbeheerders:** *1Password, NordPass, Dashlane, Bitwarden, KeePass*, enz.

TWEEFACTORAUTHENTICATIE (2FA): hoe werkt het?

We lichten toe hoe u 2FA activeert op de twee populairste platformen: Facebook en Gmail. Eigenlijk gaat het bij alle platformen zoals bij deze twee.

FACEBOOK : Klik op de drie streepjes bovenaan links, vervolgens op *Instellingen en privacy*, dan op *Instellingen*, vervolgens op *Accountcentrum*, dan op *Wachtwoord en beveiliging* en nadien op Tweestapsverificatie. Kies de methode *Verificatieapp* (installeer de app *Google Authenticator*), volg de instructies en bevestig met de code die u ontvangt om uw account te beveiligen.

GMAIL : Klik op de foto van uw Google-account, dan op *Je Google-account beheren* en vervolgens op *Beveiliging en inloggen*. Onder *Inloggen bij Google* klikt u op *Tweestapsverificatie* en kiest u de *Authenticator-app*. Open nu de app *Google Authenticator* op uw smartphone, druk op + en kies *QR-code scannen.* Om de configuratie te voltooien, tikt u de 6-cijferige code in die op uw smartphone

4 TWEEFACTORAUTHENTICATIE: een tweede en sterke afweerlinie

Zelfs als er een veiligheidsslot op de deur zit, zorgt een extra grendel voor nóg meer veiligheid. Tweefactorauthenticatie (2FA), ook wel 'tweestapsverificatie' genoemd, betekent dat er een extra goedkeuring vereist is (vaak via uw smartphone) om in te loggen.

- **Geef de voorkeur aan** authenticatie-apps (*Google Authenticator, Microsoft Authenticator*) of fysieke sleutels.
- **Vermijd zo mogelijk** een code via sms als tweede factor, want die kan door ervaren hackers worden onderschept (*SIM swapping*). Bewaar zorgvuldig de veiligheidscodes die de diverse platformen u doorsturen.

Een back-up: de levensverzekering voor uw gegevens

Nulrisico bestaat niet, zelfs niet met de allerbeste beveiliging. Een materieel defect, een menselijke fout, een cyberaanval, enz.: bij onvoorziene gebeurtenissen staat of valt het voortbestaan van uw business met een uitgekiende back-upstrategie. Omdat back-upautomatisering de menselijke factor uitschakelt, staat ze borg voor feilloze regelmaat en garandeert ze dat u altijd over de recentste gegevens kunt beschikken. Hierbij een leidraad om van back-ups een eenvoudige routine te maken.

Een robuuste back-upstrategie wordt ondersteund door 4 pijlers.

1 Automatiseren om niets te vergeten

Menselijke fouten zijn de belangrijkste oorzaak van dataverlies. Als u uw back-ups automatiseert, bent u zeker dat die met feilloze regelmaat worden gemaakt.

- **Al gehoord van *version control*?** Dankzij *version control* of versiebeheer kunt u teruggaan in de tijd en, na een foutieve verrichting of na beschadiging door een virus, een correcte versie van een document terughalen.
- **Plan regelmatig back-ups in:** waarom bijvoorbeeld niet op momenten dat u niet aan het werk bent?
- **Vergeet niet de verbinding met de externe back-ups te verbreken** zodra de back-up is voltooid.

2 De gulden '3-2-1-regel'

Deze methode is wereldwijd bekend:

- **Bewaar 3 exemplaren van uw gegevens** (het origineel + twee back-ups).
- **Op 2 verschillende dragers** (bijvoorbeeld een lokale server en een harde schijf – Opgelet: ook een harde schijf gaat niet eindeloos mee).
- **& 1 kopie *ex situ*** (in een beveiligde cloudomgeving) voor het geval er zich een fysiek schadegeval zoals een brand voordoet.

Organisatietip: gebruik de Grandfather-Father-Son- of GFS-methode. Deze rotatiestrategie organiseert uw back-ups in drie cycli: dagelijks (*zoon*), wekelijks (*vader*) en maandelijks (*grootvader*). Zo kunt u over een lange periode een historiek van uw back-ups bijhouden, terwijl de vereiste opslagruimte beperkt blijft.

3 Uw vertrouwelijke gegevens achter slot en grendel

Een gestolen back-up mag geen gegevenslek worden.

- **Encryptie:** versleutel uw back-ups stelselmatig. Zonder de juiste sleutel zijn uw bestanden onleesbaar.
- **De herstelsleutel:** dit is uw redder in nood. Bewaar de sleutel zorgvuldig in een wachtwoordbeheerder of in een fysieke kluis. Zonder de herstelsleutel kunt zelfs u niet meer aan uw data.

4 Testen vóór er problemen optreden

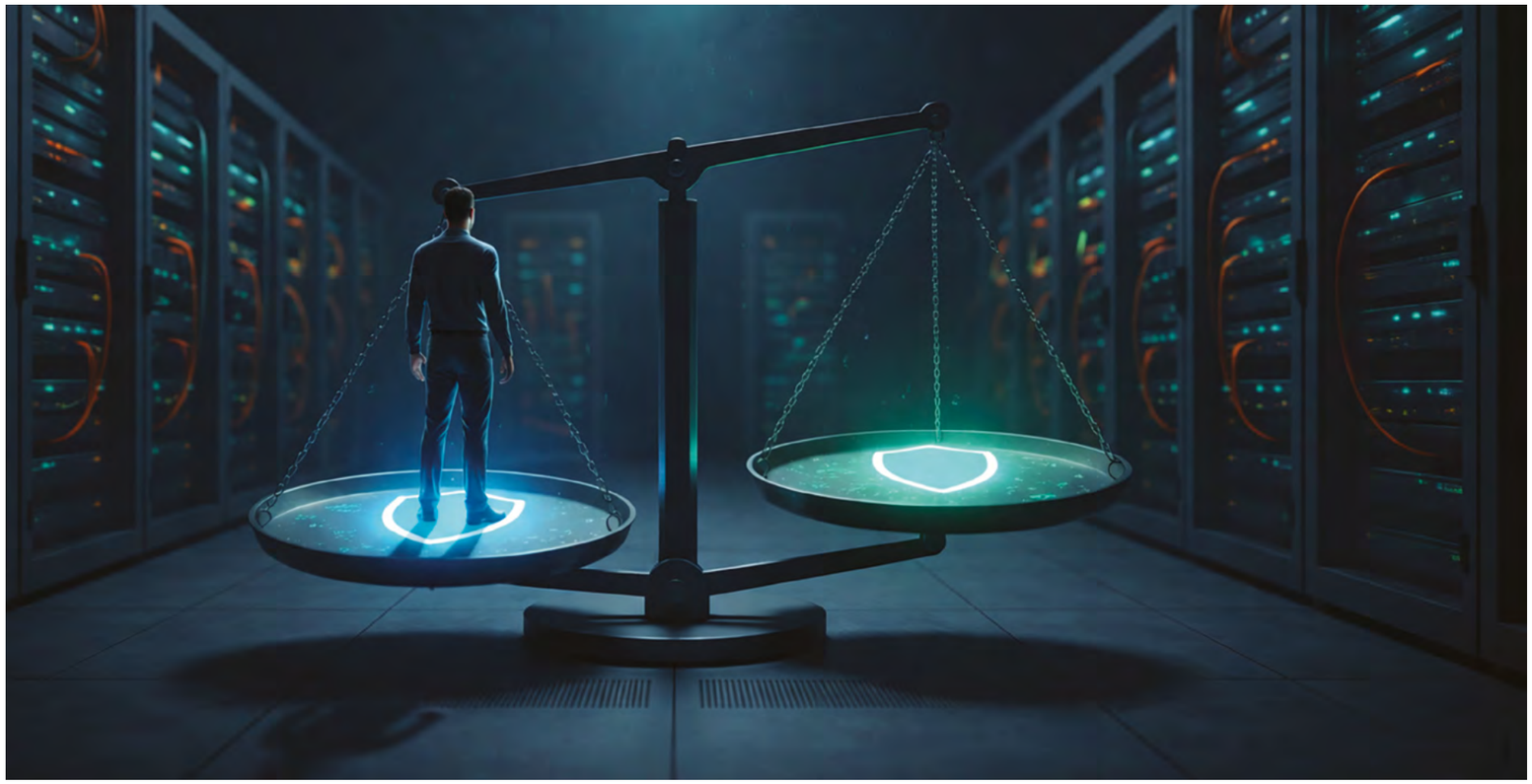
Het belangrijkste advies dat u voor ogen moet houden? Een back-up is pas nuttig als die ook echt werkt. Daarom:

- **Elk kwartaal:** probeer of u enkele willekeurige bestanden kunt herstellen.
- **Elk jaar:** simuleer een volledig herstel van uw systeem.

Het oog van de kenner: vraag aan een externe expert om uw strategie onder de loep te nemen. Een neutrale blik ziet soms veiligheidslekken die van binnenuit niet zichtbaar zijn.

Hoe kiest u een prima antivirusprogramma?

De website https://www.av-test.org/en/ werd aangemaakt door een onafhankelijk Duits onderzoekinstituut dat zich toelegt op IT-beveiliging en al meer dan 20 jaar actief is. De experts van het instituut testen op internationaal niveau de kwaliteit van diverse IT-beveiligingsproducten. Op de website vindt u een gedetailleerde vergelijking van de softwaretoepassingen, gebaseerd op strenge testprotocollen en zonder beïnvloeding door sponsors. Gebruikers kunnen, afhankelijk van hun noden (bv. bescherming voor één of meerdere toestellen), kiezen tussen gratis of betalende oplossingen.



Al gedacht aan een **superadministrator** (superbeheerder)?

Bij het downloaden van apps of software is het cruciaal dat vastligt wie die mag installeren. Door op elke computer in het bedrijf een superbeheerdersaccount aan te maken, behoudt u de totale controle over het systeem. De superadministrator beheert de kritieke bestanden, kan zonder beperkingen programma's installeren of verwijderen en configureert de rechten van de andere gebruikers.

In een gedeelde IT-omgeving – of dat nu op het werk is of thuis– voorkomt zo'n account dat onbevoegde gebruikers gevaarlijke wijzigingen doorvoeren (bv. zomaar om het even welke toepassing installeren), wat de veiligheid van het systeem ten goede komt. Zo'n account is ook cruciaal bij technische problemen, want de superadministrator kan beschadigde bestanden herstellen of kwaadaardige software verwijderen. Samen met strengere beveiligingsinstellingen, een robuust wachtwoord en een gecentraliseerd toegangsbeheer beschermt de superbeheerder het systeem tegen indringers. Toch is ook hier voorzichtigheid geboden: de toegang van de superadministrator moet goed worden beveiligd om het risico op verkeerde handelingen of ongewenste indringers maximaal te beperken.

Bij cybersecurityproblemen valt de menselijke invloed niet te onderschatten

De mens is uw beste schild tegen cyberdreigingen. Als het over cybersecurity gaat, is een periode zonder incidenten geen garantie dat er u niets meer kan overkomen. Technologische tools mogen dan al onontbeerlijk zijn, sensibilisering en alertheid – van uzelf én van uw medewerkers – vormen de eerste verdedigingslinie rond uw onderneming.

Til uw waakzaamheid naar een hoger niveau in vier stappen.

1 Voorkom MENSELIJKE FOUTEN

De mens is vaak het favoriete doelwit van hackers. Informatie is uw beste wapen om nare verrassingen te vermijden.

- **Blijf uitkijken:** raadpleeg geregeld de website Safeonweb om te weten welke vormen van phishing circuleren en praat erover met anderen.
- **Leer bij:** gebruik de praktische leidraden van het CCB om bedrog te leren herkennen.
- **Automatiseer gespecialiseerde nieuwsbrieven:** abonneer u op gespecialiseerde nieuwsbrieven zodat u incidenten niet hoeft te ondergaan, maar proactief kunt handelen.

2 Zorg dat iedereen binnen het bedrijf dezelfde REFLEXEN heeft

Beveiliging mag geen kwestie zijn van persoonlijke interpretatie. Om vermijdbare barsten in de beveiliging te dichten, is een goed gestructureerde werkwijze een must.

- **Het IT-charter:** leg duidelijke regels vast die voor iedereen gelden en die iedereen aanvaardt.
- **Leidraad met *best practices*:** een eenvoudig document met een overzichtelijke samenvatting van de dagelijkse handelingen (wachtwoorden, schermvergrendeling tijdens een gebruikerssessie, gebruik van USB-sticks)..

3 Stel een *INCIDENT RESPONSE PLAN* op (IRP)

Doet er zich toch een incident voor? Onderga het niet, pak het aan. Een *Incident Response Plan* (IRP) stelt u in staat snel en methodisch te reageren om de impact van een cyberaanval in te dijken. Een IRP is de tegenhanger van een evacuatieplan bij brand. Wat behelst een goed IRP?

- **Detectie en analyse:** snel bepalen om wat voor incident het gaat, inschatten wat de omvang is, welke systemen getroffen zijn en welke personen betrokken zijn.
- **Afbakening en opschoning:** de aangetaste systemen isoleren om te voorkomen dat het probleem zich verspreidt, kwaadaardige elementen verwijderen.
- **Herstel:** gegevens terugzetten via de beveiligde back-ups, nieuwe toestellen of systemen kopen en de activiteiten hervatten.
- **Analyse en verbetering:** het incident achteraf analyseren om de aanval te begrijpen en de beveiliging te versterken.

4 De CYBERRISICOVERZEKERING als vangnet

Nulrisico bestaat niet, zelfs niet met de beste verdediging. Een cyberrisicoverzekering is als het ware een laatste vestingmuur. De voordelen:

- dekking van exploitatieverliezen en herstelkosten;
- onmiddellijke toegang tot **experten in crisismanagement** en tot juridisch advies.

Uw eerste reflex moet regionaal zijn: daar is de meest laagdrempelige steun te vinden.

Complete leidraad voor overheidssteun op het vlak van cybersecurity (Vlaams, Brussels, federaal en Europees niveau)

Cyberaanvallen zijn helaas schering en inslag. Vandaar dat de overheid steunmaatregelen heeft uitgewerkt om ondernemingen bij te staan. Ze wil daarmee tegemoetkomen aan drie belangrijke behoeften: advies en diagnosestelling (kwetsbaarheidsaudit), opleiding (de vaardigheden van teams aanscherpen) en financiële steun (premies, leningen en fiscale stimuli).

In België is de steun aan bedrijven gespreid over verschillende beleidsniveaus. Als u de rol van elk van die niveaus begrijpt, weet u meteen waar eerst te zoeken.

- **Regionale steun:** rechtstreekse steun, subsidies, opleidingen en begeleiding (bv. VLAIO, hub.brussels).
- **Federale steun:** sensibilisering en fiscale stimuli (bv. *Safeonweb*, verhoogde fiscale aftrek).
- **Europese steun:** grootschaligere, innovatieve of samenwerkingsverbanden, vaak gericht op kmo's met een zekere maturiteit (bv. *CYSSME*, *Digital Europe Programme*)

Uw eerste reflex moet regionaal zijn, want daar is de meest laagdrempelige steun te vinden.

Steunmaatregelen in Vlaanderen

In Vlaanderen heeft het VLAIO (Agentschap Innoveren & Ondernemen) een zeer gestructureerd traject uitgestippeld, dat u begeleidt van een eerste evaluatie tot de uitrol van volledige projecten. Starten doet u met een eerste diagnose met behulp van de gratis *Cybersecurity Improvement Quickscan*. Vervolgens maakt u gebruik van de *kmo-portefeuille* om een opleiding of doelgericht advies te financieren. Voor een groot project stapt u tot slot (via het VLAIO) in een *Cybersecurity Improvement Trajectory*, dat Vlaamse kmo's begeleidt bij het analyseren en invoeren van maatregelen zoals sterke authenticatie of back-ups. Het project moet 8.500 tot 35.000 euro kosten. De tussenkomst bedraagt 50%.

Voor wie liever niet bij de bank gaat aankloppen voor financiering, is er de winwinlening: hierbij leent een particulier geld aan een onderneming. De kredietverstrekker zelf heeft recht op een fiscaal voordeel.

U wil uw medewerkers een opleiding laten volgen? De *kmo-portefeuille* financiert erkende opleidingen (a rato van 45% voor kleine ondernemingen).

Steunmaatregelen in het Brussels Hoofdstedelijk Gewest

Het Brusselse model is simpel en logisch: u begint met *Digital First Coaching* (via hub.brussels) om een gratis diagnose te krijgen en maakt vervolgens gebruik van de *digitaliseringspremie* om de aanbevolen oplossingen rechtstreeks te financieren.

De *digitaliseringspremie* van het Brussels Hoofdstedelijk Gewest ondersteunt de aankoop van IT-apparatuur, software (CRM, cloudtoepassingen) en cybersecuritytools (firewall, antivirus). De tussenkomst bedraagt 25% tot 70%, afhankelijk van de grootte van de onderneming.

Ook in Brussel kunt u een 'alternatieve' lening aangaan als u niet bij een bank wenst aan te kloppen. Via de *proxilening* kunnen particulieren (familie, kennissen, klanten) geld lenen aan een Brussels bedrijf in ruil voor een fiscaal voordeel (belastingkrediet).

Wil u uw medewerkers een cursus laten volgen? Actiris betaalt tot 100% van de kosten van ICT-cursussen (informatie- en communicatietechnologie). U kunt ook terecht bij Digitalcity.brussels, een opleidings- en tewerkstellingspool voor digitale beroepen.

Hoe weet ik onder welk Gewest ik val?

Dat hangt af van de exploitatiezetel of de maatschappelijke zetel van uw onderneming. Om voor steun in aanmerking te komen, moet uw onderneming ingeschreven zijn bij de Kruispuntbank van Ondernemingen (KBO) en actief zijn in het desbetreffende Gewest (Vlaanderen, Brussel of Wallonië).

Steunmaatregelen op federaal niveau

Op dit niveau zijn er twee belangrijke initiatieven.

Sensibilisering via *Safeonweb* en het Centrum voor Cybersecurity Belgium (CCB): praktisch advies, veiligheidswaarschuwingen en preventietools voor alle burgers en ondernemingen.

Fiscale stimulus: los van de regionale premies staat de federale overheid een verhoogde fiscale aftrek toe voor digitale investeringen, waaronder investeringen in data- en netwerkbeveiliging (via de FOD Financiën).

Steunmaatregelen op Europees niveau

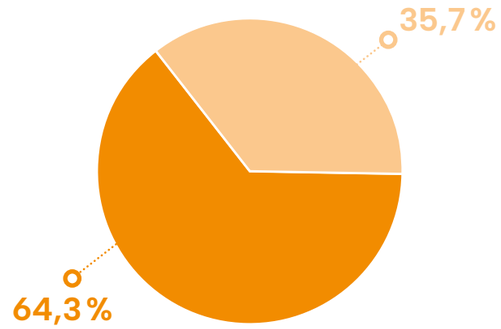
Deze vormen een aanvulling op de eerdergenoemde initiatieven en focussen op algemene sensibilisering en grootschaligere projecten. Een voorbeeld is *CYSSME* (*Cybersecurity for SMEs*), een stappenaanpak die volledig gratis is voor kmo's met minder dan 250 medewerkers en die behalve een audit ook een actieplan en begeleiding door experts omvat. De ideale oplossing voor bedrijven die hun cybersecuritystrategie van a tot z willen structureren met kwaliteitsvolle omkadering. *CYSSME* biedt een gestructureerd begeleidingstraject (audit en tools) en tot 20.000 euro aan financiering zonder rechtstreekse kost voor de geselecteerde onderneming. Voor ambitieuzere researchprojecten zijn er de programma's *Digital Europe* en *Horizon Europe*.

Uw mening telt

Wij hebben een tevredenheidsenquête opgesteld voor de zelfstandigen en de kmo's die deelnamen aan *Cyber Challenge*, om te peilen naar hun ervaringen en naar de impact van het project. De feedback die wij aldus van de deelnemers ontvingen, stelt ons in staat de kwaliteit van de aangeboden begeleiding, de relevantie van de aanbevelingen rond cybersecurity en het nut van de aangereikte tools te evalueren. De ingezamelde antwoorden geven ook aan welke punten voor verbetering vatbaar zijn en hoe we het project kunnen bijsturen om het nóg beter te laten aansluiten bij de echte noden van ondernemers die geconfronteerd worden met digitale uitdagingen en cyberrisico's.

Uit de eerste resultaten van de enquête blijkt dat de deelnemers uiterst tevreden waren over het programma. **Ruim 60% van de respondenten zou het zonder aarzelen aanbevelen aan andere zelfstandigen**, wat aantoont hoe interessant en relevant de door *Cyber Challenge* verstrekte begeleiding is.

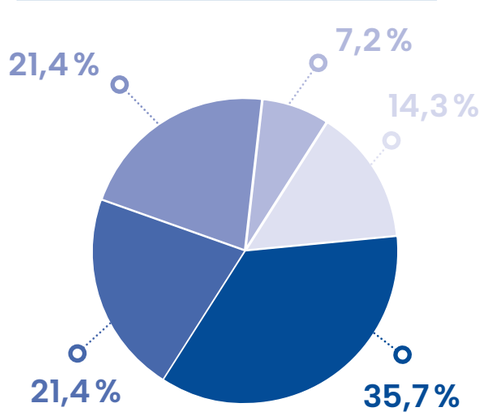
Zou u dit programma aanbevelen aan andere zelfstandigen?



Deze feedback sterkt ons in een van de belangrijkste doelstellingen van dit project: zorgen dat zelfstandigen en kmo's een beter zicht hebben op de digitale risico's waaraan ze zijn blootgesteld en hen aanmoedigen concrete maatregelen te nemen om hun digitale omgeving te beveiligen.

De bevraging leert ook dat het programma een impact heeft op de sensibilisering van ondernemers rond de uitdagingen op het vlak van cybersecurity. **Meerdere deelnemers geven aan dat ze zich bewust zijn geworden van hun digitale kwetsbaarheden en dat ze stappen hebben gezet – of hebben overwogen – om hun business en hun data beter te beschermen.**

Naar aanleiding van het programma…:



Wij danken alle deelnemers die tijd hebben gemaakt om hun ervaringen te delen.
Hun feedback is voor ons cruciaal om het project voortdurend te verbeteren en om onze begeleiding van ondernemers bij het beschermen van hun business verder te versterken.

De cyberscan

Cyberaanvallen komen steeds vaker voor in onze gedigitaliseerde wereld. Geen enkele kmo of zelfstandige is immuun. Meer dan één op de vijf Belgische kmo's is al het slachtoffer geweest van een IT-beveiligingsincident!

Daarom heeft de FOD Economie in 2022 de Cyberscan gelanceerd.

Dit hulpmiddel is speciaal ontworpen voor kleine bedrijven en zelfstandigen en is beschikbaar in een begrijpbare taal. Het biedt u de mogelijkheid om uw niveau van cyberbeveiliging te evalueren aan de hand van acht modules:

1. INVENTARISEREN en ANALYSEREN: bekijk hoe u er voor staat;
2. Over passende PROCEDURES beschikken: maak een plan;
3. SENSIBILISEREN: uw plan in de praktijk;
4. SLEUTELROLLEN toewijzen: verdeel de verantwoordelijkheden;
5. VERDEDIGINGSSYSTEEM: zet de juiste tools in;
6. OPSLAAN: back-ups maken;
7. UPDATEN: blijf voorbereid;
8. EVALUEREN: zet uw beschikbare middelen optimaal in.

Voor elk van deze modules ontvangt u advies dat is afgestemd op uw situatie, een checklist en een downloadbare handleiding om deze tips in de praktijk te brengen.

Laat u niet misleiden door hackers, voer de Cyberscan uit op https://economie.fgov.be/nl/cyberscan !

STARTER | ZELFSTANDIGE | HANDELAAR | KMO | VRIJ BEROEP

NSZ begeleidt ALLE zelfstandigen bij al hun keuzes

INDIVIDUELE VERDEDIGING & **COLLECTIEVE VERDEDIGING**

WIJ NEMEN DE RECHTEN EN DE BELANGEN VAN ELKE ZELFSTANDIGE EN ELKE BEDRIJFSLEIDER TER HARTE

- JURIDISCH, SOCAAL EN FISCAAL ADVIES
- JURIDISCHE BIJSTAND
- INNING VAN SCHULDEN
- PERSONEELS-PROBLEMEN
- CONTRACTEN OP MAAT
- HULP AAN STARTERS
- SUBSIDIES
- GDPR-TOOLS
- MAGAZINE
- INFOSESSIES EN WEBINARS
- NETWORKING
- KORTINGEN EN VOORDELEN
- PROGRAMMA DIGITAL COMMERCE
- PROGRAMMA BECYBERSAFE
- PROGRAMMA PROCOMMERCE

En nog véél meer!

CONTACT?
Wij zijn bereikbaar op **02 217 29 28** of via **info@nsz.be.**
Een van onze medewerkers zal u te woord staan om al uw vragen te beantwoorden. Via de QR-code hiernaast kunt u een kijkje nemen op onze website.
Aangename kennismaking!

nsz neutraal syndicaat voor zelfstandigen

www.nsz.be @NSZ_be @NSZ_be
Neutraal Syndicaat voor Zelfstandigen