



SECTORGIDS

Modesector

De modemaak- en kledingsector is een innovatieve en veelzijdige industrie die steeds sterker leunt op digitale systemen. Van ontwerpsoftware en digitale productontwikkeling tot voorraadbeheer, e-commerce en internationale logistiek: digitalisering heeft de sector sneller, transparanter en efficiënter gemaakt. Maar die digitale vooruitgang brengt ook nieuwe risico's met zich mee. Daarom is cybersecurity een essentieel onderdeel geworden van elke moderne mode- en kledingonderneming.

Inhoudstafel

Digitale vooruitgang vraagt om gerichte cyberweerbaarheid	3
Cyberveiligheid in de modesector	4
Podcasttip	7
1. Inventariseren	8
2. Update	9
3. Multi-factor	10
Met de juiste partij in zee	11
Getuigenis: Marylise & Rembo Fashion Group	12
4. Isoleren	16
Ontdek de lespakketten	17
5. Bewustzijn	18
6. Anti-virus	19
Experten aan het woord	20
7. Toegang op afstand	21
Getuigenis: Broothaers NV	22
Experten aan het woord	26
Cyberveiligheid hoeft niet complex of duur te zijn	27
8. Wargame	28
Cyberveiligheid: is het nodig voor jouw onderneming?	29
NIS2-richtlijn, wat betekent dit voor mijn onderneming?	30
Safeonweb@work	31
Conclusie	32

Deze gids kwam tot stand met de steun van de FOD Economie en is gefinancierd door de Europese Unie & NextGenerationEU.



Digitale vooruitgang vraagt om gerichte cyberweerbaarheid

Met deze reeks sectorgerichte gidsen willen we ondernemingen helpen om de kansen van digitalisering ten volle te benutten, zonder de gevaren van cyberdreigingen uit het oog te verliezen. Want wie vandaag digitaal onderneemt, moet ook digitaal weerbaar zijn.

We leven in een tijdperk waarin digitalisering niet langer optioneel is, maar essentieel om als onderneming mee te blijven draaien, te groeien en te innoveren. Technologie maakt onze bedrijven sneller, efficiënter en beter verbonden dan ooit tevoren. Van slimme toepassingen en cloudoplossingen tot mobiele werkomgevingen en geautomatiseerde processen: digitalisering is de motor achter modern ondernemerschap.

Maar diezelfde digitalisering maakt bedrijven ook kwetsbaarder. Cyberdreigingen zijn de afgelopen jaren explosief toegenomen, in volume én in complexiteit. Cybercriminelen worden steeds professioneler en hun aanvallen steeds gericht.

Geen enkele sector ontsnapt daaraan, en ook kleine en middelgrote ondernemingen worden steeds vaker het doelwit. Een phishingmail, een gehackte leverancier of een lek in verouderde software kan al voldoende zijn om volledige bedrijfsprocessen lam te leggen of gevoelige data bloot te stellen.

Cybersecurity is dus geen louter technisch verhaal meer, en al zeker geen zorg voor enkel de IT-afdeling. Het is een strategisch thema dat op elk niveau binnen de organisatie aandacht verdient, van de werkvloer tot het management.

Want de impact van een cyberincident raakt alle lagen van het bedrijf: financieel, operationeel én reputatiegewijs.

Met deze sectorgidsen willen we bedrijven ondersteunen in hun zoektocht naar meer digitale weerbaarheid. Elke sector kent immers zijn eigen processen, kwetsbaarheden en digitale ecosystemen. Door cybersecurity sectorspecifiek te benaderen kunnen we praktischer adviseren, gericht waarschuwen en effectiever oplossingen aanreiken.

Dit initiatief is in het leven geroepen om bewustzijn rond cybersecurity te vergroten, maar vooral om actie te stimuleren. We willen ondernemingen helpen om niet alleen risico's te herkennen, maar ook de juiste stappen te zetten, van preventie tot reactie. Elke gids bevat daarom een combinatie van toegankelijke uitleg, realistische risico's en praktische aanbevelingen, afgestemd op de sector waarvoor ze is bedoeld.

Samen bouwen we zo aan een veerkrachtige, veilige en toekomstgerichte digitale economie, waarin ondernemers met vertrouwen kunnen blijven innoveren.

Cyberveiligheid in de modesector

De B2B-distributie en productieateliers in de mode- en kledingsector digitaliseert in sneltempo: collecties worden online gelanceerd, bestellingen verlopen via e-commerceplatformen en zowel retailers als distributeurs verwachten een foutloze digitale keten. Merken verzamelen en verwerken grote hoeveelheden gevoelige gegevens, van klantprofielen en betalingsinformatie tot productie- en logistieke data. Dat biedt efficiëntiewinsten, maar maakt de sector tegelijk een aantrekkelijk doelwit voor cybercriminelen.

Cybersecurityrisico's

Intellectueel eigendom (IP) diefstal

Modeontwerpen, productieschema's en innovaties zijn waardevolle activa. Cybercriminelen kunnen proberen deze te stelen voor concurrentievoordeel of illegale reproductie.

Ransomware-aanvallen

Ransomware-aanvallen kunnen leiden tot stillegging van productielijnen en distributiekanaalen, waardoor bedrijven losgeld moeten betalen om weer toegang te krijgen tot hun systemen en gegevens.

Supply chain-aanvallen

De mode-industrie werkt nauw samen met diverse leveranciers en partners. Een zwakke schakel in de keten kan leiden tot een bredere compromittering van systemen en gevoelige gegevens.

Gegevensdiefstal en -verlies

Bedrijven in deze sector verzamelen en verwerken grote hoeveelheden klantgegevens, waaronder betalingsinformatie en koopgedrag. Diefstal of verlies van deze gegevens kan leiden tot aanzienlijke schade aan de reputatie en juridische consequenties.

Phishing en social engineering

Medewerkers kunnen het doelwit zijn van phishing-aanvallen en social engineering tactieken, wat kan leiden tot ongeautoriseerde toegang tot systemen of financiële verliezen.

Beveiliging van mobiele apparaten

Werknemers gebruiken vaak mobiele apparaten voor communicatie en gegevensbeheer, zowel in fabrieken als in distributiecentra. Deze apparaten zijn kwetsbaar voor aanvallen als ze niet goed beveiligd zijn.

Verouderde software en systemen

De sector maakt gebruik van gespecialiseerde software voor ontwerp, productie en logistiek, die niet altijd regelmatig wordt bijgewerkt, waardoor er kwetsbaarheden ontstaan.

E-commerce bedreigingen

Online winkels en e-commerce platforms zijn kwetsbaar voor cyberaanvallen zoals creditcardfraude, DDoS-aanvallen, en skimming van betalingsgegevens.



Praktische maatregelen voor een betere cyberhygiëne

Het goede nieuws: met gerichte maatregelen kunnen bedrijven in de sector hun weerbaarheid aanzienlijk verhogen. Hieronder een overzicht van concrete aanbevelingen:

- **Houd systemen up-to-date:** Installeer regelmatig beveiligingsupdates, ook voor IoT-apparaten.
- **Gebruik sterke toegangscontrole:** Implementeer multi-factor authenticatie en beperk toegang tot gevoelige data.
- **Versleutel gevoelige informatie:** Zorg voor encryptie van data, zowel in rust als tijdens overdracht.
- **Investeer in awareness:** Train medewerkers in het herkennen van phishing en andere cyberdreigingen.
- **Beheer mobiele toestellen centraal:** Gebruik mobiele device management om dataverlies bij verlies of diefstal te voorkomen.
- **Voorzie een incident response plan:** Bereid je voor op een aanval met een getest stappenplan.
- **Zorg voor ketenveiligheid:** Stel eisen aan leveranciers en werk samen rond beveiliging via contracten, audits en training.
- **Bescherm je e-commerce:** Implementeer sterke beveiligingsmaatregelen voor e-commerce platforms, zoals SSL-certificaten, tokenization van betalingsgegevens, en regelmatige beveiligingsscan's.
- **Implementeer Data Loss Prevention (DLP):** Gebruik DLP-oplossingen om te voorkomen dat gevoelige gegevens ongeoorloofd worden gedeeld of gelekt.

Cyberveiligheid is geen bijzaak meer, maar een noodzaak voor elke speler in de transport- en logistieke sector. Door te investeren in preventie, bewustwording en samenwerking binnen de keten, versterken bedrijven hun digitale weerbaarheid en blijven ze operationeel én competitief in een steeds digitalere wereld.



Enkele praktische maatregelen uitgelicht


- 1 Inventariseren**
Een doeltreffende cybersecurity start met een overzicht van alle hardware en software binnen je bedrijf.
- 2 Update**
Regelmatige updates beschermen je systemen tegen kwetsbaarheden en zorgen voor een optimale veiligheid.
- 3 Multi-factor (MFA)**
Met MFA bescherm je je accounts beter, zelfs als je wachtwoord wordt buitgemaakt.
- 4 Isoleren**
Isolatie beperkt risico's door kwetsbare systemen los te koppelen van je netwerk.
- 5 Bewustzijn**
Menselijke fouten blijven een groot cyberrisico, dus is bewustmaking cruciaal om veilig gedrag te stimuleren.
- 6 Anti-virus**
Antivirussoftware vormt een essentiële eerste verdedigingslinie tegen malware en cyberaanvallen.
- 7 Toegang op afstand**
Toegang op afstand biedt flexibiliteit, maar vraagt om sterke beveiliging om misbruik en datalekken te voorkomen.
- 8 Wargame**
Een simulatie van een cyberaanval helpt je inschatten hoe goed je bent voorbereid op een echte digitale crisis.


Podcasttip

De UNIZO Podcasts zijn er voor ondernemers die op zoek zijn naar inspiratie, inzichten en praktische tips, op het moment dat het hen past. Of je nu onderweg bent, tussen twee afspraken door wat tijd hebt of tijdens het werk even wil bijleren: de podcasts van UNIZO zijn jouw ideale compagnon.

Luister naar boeiende verhalen van collega-ondernemers, ontdek slimme strategieën en krijg advies van experts die weten wat er leeft in het ondernemerschap. Kort, krachtig en altijd relevant voor jouw zaak.

 [Spotify](#)

 [Apple Music](#)

 [Youtube](#)



Webinartip

Herbekijk al onze inspirerende webinars rond digitalisering – van phishingtrends en welke subsidies je kan inzetten tot veilig omgaan met data en AI in je onderneming.

Onze experts en ondernemers delen concrete tips, handige tools en hun eigen ervaringen. Ideaal voor zelfstandigen en KMO's die hun digitale kennis willen versterken op hun eigen tempo.

<https://www.unizo.be/berichten/nieuws/webinars-voor-digitale-ondernemers>



1. Inventariseren

Een goede cybersecuritystrategie begint bij een helder overzicht van je digitale omgeving. Je kunt pas beschermen wat je kent. Daarom is het essentieel om eerst in kaart te brengen welke hardware en software je precies gebruikt binnen je onderneming. Die inventaris vormt de basis voor gerichte en efficiënte beveiligingsmaatregelen.

1 Wat?

Maak een lijst van alle hardware die binnen je onderneming aanwezig is, zoals pc's, servers, laptops, mobiele toestellen, NAS-schijven (harde schijven die autonoom verbonden zijn met je netwerk) en eventuele machines indien relevant. Inventariseer de software die je gebruikt, inclusief zowel geïnstalleerde programma's op je pc's als web-based (cloud) toepassingen, en vermeld daarbij ook de software die je niet meer gebruikt.

3 Hoe?

Kleinere organisaties kunnen dit handmatig aanpakken. Gebruik een spreadsheet en noteer welke toestellen je hebt en welke software daarop staat. Zorg ervoor dat je ook aangeeft wat cruciaal is voor je bedrijf en wat minder belangrijk is. Grotere ondernemingen kunnen deze inventarisatie laten uitvoeren met een geautomatiseerde scan, eenmalig of periodiek, om altijd up-to-date te blijven.

2 Waarom?

Het begint allemaal met inzicht: als je weet wat je moet beschermen, kun je ook bepalen wat de moeite waard is om te verdedigen. Niet alles hoeft beschermd te worden; je kunt er bewust voor kiezen om bepaalde zaken niet te verdedigen, zolang je die keuze maar weloverwogen maakt.

Meer info

Een doeltreffende cybersecurity start met een overzicht van alle hardware en software binnen je bedrijf.

 **Module 1d - Je zaak beschermen tegen hackers: Hoe begin je eraan**

www.unizo.be/CS4ZO-opleidingsprogramma

2. Update

Het updaten van software is essentieel voor de veiligheid en prestaties van je systemen. Updates verhelpen kwetsbaarheden en voorkomen dat hackers deze misbruiken. Ze zorgen ook voor betere functionaliteit en stabiliteit. Door regelmatig te updaten, bescherm je je systemen tegen bedreigingen en houd je je software optimaal werkend.

1 Wat?

Zorg ervoor dat je security updates zo snel mogelijk uitvoert, bij voorkeur automatisch. Dit geldt niet alleen voor je besturingssystemen, zoals Windows, maar ook voor alle programma's en machines die je gebruikt, machines worden vaak over het hoofd gezien. Controleer daarnaast of al je programma's nog te updaten zijn. Soms is de software te oud of kan je hardware de nieuwste versie niet aan.

3 Hoe?


Kleinere organisaties kunnen dit handmatig doen. Gebruik de inventaris uit punt 1 en controleer wekelijks of tweewekelijks al je software om updates uit te voeren. Grotere bedrijven zouden dit proces moeten automatiseren en regelmatige scans uitvoeren om zeker te zijn dat alle software up-to-date is.

2 Waarom?

Software wordt door mensen geschreven, en mensen maken fouten. Daardoor bevat software altijd fouten. Security updates herstellen deze fouten. Als je die updates niet uitvoert, kunnen hackers deze kwetsbaarheden (bugs) misbruiken om controle te krijgen over jouw apparaten.

Meer info

Regelmatige updates beschermen je systemen tegen kwetsbaarheden en zorgen voor optimale veiligheid.

 **Module 4a - Malware**
Module 4b - Ransomware

www.unizo.be/CS4ZO-opleidingsprogramma

3. Multi-factor

Multi-factor authenticatie (MFA) biedt een essentiële extra beveiligingslaag door naast een wachtwoord een tweede vorm van identificatie te vereisen, zoals een sms-code of biometrische scan. Dit maakt het voor onbevoegden veel moeilijker om toegang te krijgen, zelfs bij een gestolen wachtwoord. MFA versterkt de bescherming van je gevoelige informatie en is onmisbaar in de strijd tegen geavanceerde cyberdreigingen.

1 Wat?

Multi-factor authenticatie (MFA) voegt een extra beveiligingslaag toe bovenop je wachtwoord. Dit kan een SMS-code of een code in je authenticator-app zijn.

Je kunt MFA instellen voor het opstarten van je pc en voor toegang tot je meest kritische applicaties zoals je mailbox, administratie of machineconfiguratie.

3 Hoe?


Je kunt zelf kiezen welke vorm van multi-factor authenticatie je gebruikt. Authenticator-apps zijn veiliger dan SMS-codes. Biometrische beveiliging op je smartphone is meestal nog beter dan een authenticator-app. Zelfs de minst sterke optie, zoals een SMS-code, biedt echter een waardevolle extra beveiligingslaag bovenop je wachtwoord. Zorg ervoor dat je dit toepast op alle belangrijke software in je onderneming en zeker bij het opstarten van je pc en het openen van je mailbox.

2 Waarom?

Multi-factor authenticatie (MFA) voegt een extra beveiligingslaag toe bovenop je wachtwoord. Dit kan een SMS-code of een code in je authenticator-app zijn. Je kunt MFA instellen voor het opstarten van je pc en voor toegang tot je meest kritische applicaties zoals je mailbox, administratie of machineconfiguratie.

Meer info

Met MFA bescherm je je accounts beter, zelfs als je wachtwoord wordt buitgemaakt.

 [Module 3a - Paswoorden](#)
[Module 3b - 2-Factor-Authenticatie](#)

www.unizo.be/CS4ZO-opleidingsprogramma



Met de juiste partij in zee!

Een goede IT-partner is essentieel voor elk bedrijf. Technologie speelt een cruciale rol in dagelijkse operaties en strategische keuzes. Een betrouwbare IT-partner zorgt niet alleen voor een stabiele infrastructuur en dataveiligheid, maar helpt ook bij het volgen van technologische evoluties en het tijdig upgraden van systemen. Zo blijf je als bedrijf efficiënt, veilig én klaar voor groei.

Wat je zelf doet, doe je niet altijd beter!

Een goede IT-partner zorgt ervoor dat je bedrijf mee is met de nieuwste technologieën en best practices. Ze volgen de IT-markt nauwgezet, adviseren over relevante innovaties en helpen je om verouderde systemen tijdig te upgraden. Zo werk je steeds met betrouwbare en efficiënte oplossingen die je helpen om kosten te besparen, productiviteit te verhogen en je onderneming klaar te stomen voor groei.

Een sterke IT-partner zorgt voor een stabiele infrastructuur, optimale beveiliging en helpt je bedrijf mee te groeien. Ze bieden proactieve ondersteuning, volgen technologische evoluties op en adviseren strategisch, zodat jij efficiënter werkt en klaar bent voor de toekomst.

Bovendien bieden ze proactieve ondersteuning. In plaats van te wachten tot er iets misloopt, detecteren en verhelpen ze problemen op voorhand. Dit voorkomt stilstand en zorgt ervoor dat je bedrijfsprocessen vlot blijven draaien.

Cyberveiligheid is een ander speerpunt. IT-partners beschermen je systemen met up-to-date beveiligingsmaatregelen, voeren regelmatige controles uit en bieden trainingen aan voor medewerkers. Zo vergroot je de digitale weerbaarheid van je hele organisatie.

Tot slot zijn ze meer dan alleen technische hulp, een goede IT-partner is ook een strategische sparringpartner. Ze denken mee over de lange termijn en helpen je om technologie slim in te zetten in functie van je bedrijfsdoelen.

Getuigenis

Marylise & Rembo Fashion Group



Marylise & Rembo Fashion Group

Marylise & Rembo Fashion Group is een echt familiebedrijf dat inmiddels aan de vierde generatie toe is. Het wordt vandaag geleid door zus en broer Chiara en Cedric De Vlieger. Het bedrijf is gespecialiseerd in bruidsmode en omvat drie merken: Marylise, Rembo en Carta Branca. De groep verkoopt niet rechtstreeks aan bruiden, maar werkt samen met geselecteerde bruidsboetieks.

“Aangezien de kosten vandaag sterk onder druk staan, biedt digitalisering een antwoord om processen te optimaliseren en competitief te blijven.”

Wat betekent digitalisering binnen jullie bedrijf?

Digitalisering is voor ons van groot belang. Omdat we een eigen productieatelier hebben, is efficiënt werken essentieel. Digitalisering helpt ons om verbeterpunten in onze productieprocessen te identificeren en zo efficiënter te werken. Aangezien de kosten vandaag sterk onder druk staan, biedt digitalisering bovendien een antwoord om processen te optimaliseren en competitief te blijven.

Is jullie onderneming actief in de cloud?

Zeker. Met een hoofdkantoor in Antwerpen en een productieatelier in Portugal zijn we constant onderweg. We

opereren bovendien in meerdere landen. De cloud maakt het mogelijk om overal toegang te hebben tot onze documenten en software, waardoor we op eender welke locatie efficiënt kunnen werken.

Hoe belangrijk is cybersecurity in jullie bedrijf?

Cybersecurity is voor ons zeer belangrijk. We werken met vertrouwelijke informatie en willen die optimaal beschermen. Daarom werken we samen met externe specialisten die ons personeel opleiden, testen en voorzien van gerichte trainingen rond cybersecurity.





Cedric De Vlieger
Marylise & Rembo Fashion Group

Wat is de belangrijkste reden om te werken in de cloud?

Onze medewerkers zijn zich ervan bewust dat ze waakzaam moeten zijn voor risico's, maar het blijft belangrijk om hen voortdurend te blijven sensibiliseren. Cyberdreigingen evolueren snel, dus blijvende alertheid is essentieel.

AI, we kunnen er niet omheen. Hebben jullie hier al stappen ondernomen?

AI vindt stilaan zijn weg binnen ons bedrijf. We implementeren het stap voor stap en zien vooral dat onze marketingafdeling AI al dagelijks inzet in hun werk.

Zijn jullie als onderneming bewust van de mogelijke risico's van AI?

Ja, we zijn ons bewust dat AI risico's met zich meebrengt. Als creatief bedrijf is het belangrijk dat we onze eigen ontwerpen beschermen en AI ondersteunend inzetten, zonder dat het creatieve proces wordt overgenomen. Daarom sensibiliseren we medewerkers ook op dat vlak.

Wat is de belangrijkste reden om AI te gebruiken?

AI is voor ons een logische volgende stap binnen de digitalisering. We verzamelen enorm veel data en AI kan ons in de toekomst helpen om die data te analyseren en er de juiste conclusies uit te trekken. Dat biedt veel kansen voor verdere optimalisatie.

Hoe zie je de toekomst van Marylise & Rembo Fashion Group en de impact van digitalisering?

Digitalisering en AI zullen in de toekomst alleen maar belangrijker worden. Op lange termijn zie ik vooral een verdere evolutie in onze productieprocessen, waarbij we steeds meer datagedreven gaan werken. Met behulp van AI kunnen we inzichten sneller interpreteren en beter onderbouwde beslissingen nemen, wat onze werking alleen maar zal versterken.

Ga voor een strategische compagnon de route!

Kris Oversteyns
Mobitel IT

Wat is het belang van een IT partner voor jullie onderneming?

Wij zijn een creatief bedrijf en focussen graag op onze kernactiviteiten. Daarom is het belangrijk om te kunnen rekenen op een betrouwbare IT-partner die ons ondersteunt bij IT-beslissingen en ons ontzorgt in de dagelijkse IT-werking. Mobitel IT neemt die rol op, zodat wij ons volledig kunnen concentreren op wat we het beste doen: creëren.

Wat verwachten jullie van een IT-partner?

Voor ons is het belangrijkste dat een IT-partner ons volledig kan ontzorgen. We beschikken niet over alle nodige technische kennis intern, dus een vertrouwensrelatie is cruciaal om de juiste beslissingen te kunnen nemen en uitdagingen op IT-vlak efficiënt aan te pakken.

Wat is de impact van de samenwerking met Mobitel IT?

Onze samenwerking met Mobitel IT is zeer positief. Ze zijn altijd bereikbaar en denken mee bij elke uitdaging. Zo kunnen problemen snel worden opgelost en blijven onze processen vlot draaien.

Wie is Mobitel IT?

Kris Oversteyns, Senior Sales Manager bij Mobitel IT: Wij verzorgen de volledige



IT-ondersteuning voor kmo's, zoals Marylise & Rembo Fashion Group. Ik ben verantwoordelijk voor de verkoop van IT-oplossingen en werk samen met onze telefonie-experts om totaaloplossingen te bieden, zowel on-premise als cloudoplossingen, zoals bij Marylise & Rembo Fashion Group.

Hoe verloopt de samenwerking tussen Mobitel IT en Marylise & Rembo Fashion Group?

We werken al sinds 2002 samen met Marylise. In 2015 maakten we samen de overstap naar de cloud, wat zeer succesvol bleek. Tien jaar later kunnen we zeggen dat Marylise & Rembo Fashion Group een van de pioniers is binnen de oplossingen die ClearMedia en Mobitel aanbieden.

We werken op basis van een all-in-bijstandsovereenkomst: klanten kunnen voor al hun IT-problemen en vragen bij ons terecht. Of het nu gaat om een defecte printer of een serverprobleem, één adres, Mobitel IT, en wij nemen alles van A tot Z op.

4. Isoleren

Isolatie voorkomt dat één zwak punt je hele netwerk in gevaar brengt. Koppel verouderde of slecht beveiligde systemen los, beperk hun internettoegang en houd ze weg van je dagelijkse werkomgeving. Zo bescherm je ook je cruciale systemen beter tegen hackers.

1 Wat?

Zorg dat je onderneming zoveel mogelijk uit gescheiden 'eilandjes' bestaat. Koppel PC's die niet per se in hetzelfde netwerk hoeven te zitten of via software die controle neemt over de machines, los. Software of machines die je niet up-to-date kunt houden of niet kunt beveiligen met multifactor authenticatie, moeten ook losgekoppeld worden van de rest.

3 Hoe?

Start met een inventarisatie: welke software of hardware is moeilijk te beveiligen door bv. gebrek aan updates of MFA? Isoleer deze zwakke schakels en zorg dat ze niet bereikbaar zijn vanaf je gewone pc en beperk hun internettoegang. Pas dit isolatieprincipe ook toe op je cruciale systemen, zoals machines, om ze extra te beschermen tegen hackers.

2 Waarom?

Een hacker zal altijd op zoek gaan naar de zwakste schakel en via die route proberen door te dringen tot de kritieke onderdelen van je onderneming. Soms heb je geen keuze en moet je oude machines behouden of kun je bepaalde software niet beveiligen met multi-factor authenticatie. Dit zijn je zwakke schakels. Door deze onderdelen los te koppelen van de rest van je systeem, voorkom je dat ze de rest van je bedrijf kunnen 'besmetten'.

Meer info

Isolatie beperkt risico's door kwetsbare systemen los te koppelen van je netwerk?



Module 1b - Veilig omgaan met je PC
Module 4c - Datadiefstal

www.unizo.be/CS4ZO-opleidingsprogramma

Ontdek de lespakketten

CS4ZO – CyberSecurity voor Zelfstandige Ondernemers is een initiatief van UNIZO dat zelfstandigen en kmo's helpt om zich beter te wapenen tegen cyberdreigingen. Het programma sluit aan bij de Belgische Cybersecurity Strategie en richt zich op een stapsgewijze aanpak, aangepast aan de noden van zowel kleine zelfstandigen als grotere kmo's.

Het programma biedt gratis videolessen, podcasts, microlearnings en handige gidsen over de belangrijkste thema's in cybersecurity.

De basis

- De KMO. Doelwit van hackers.
- Veilig omgaan met je PC.
- Veilig omgaan met je smartphone.
- Je zaak beschermen tegen hackers. Hoe begin je eraan?

Phishing

- Standaard phishing.
- Geavanceerd phishing.
- Hacking in de praktijk. Datadiefstal.

Paswoorden

- Paswoorden.
- Multi-factor authenticatie.
- Hacking in de praktijk.
- Factuurfraude.

Malware

- Malware.
- Ransomware.
- Datadiefstal.
- Hacking in de praktijk.
- Ransomware.

Alles rond je onderneming

- Aanvallen op de toeleveringsketen.
- Thuis - Werk.
- Wifi - Cloud - VPN.
- Mijn website.

Better safe than sorry

- Beveiligingsmonitoring.
- Maatregelen. Alles op een rij.
- Cyber Wargame.



5. Bewustzijn

De mens is vaak de zwakste schakel in cybersecurity. Een ondoordachte klik of slordig wachtwoord kan volstaan om een hacker binnen te laten. Cybercriminelen mikken breed en hopen dat iemand ergens een fout maakt, en dat kan evengoed bij jou op kantoor zijn. Daarom is bewustmaking essentieel: leg in klare taal uit waar medewerkers op moeten letten én waarom. Alleen wie het belang begrijpt, is bereid om veilig te werken, ook als dat iets minder comfortabel is.

1 Wat?

De mens wordt vaak gezien als de zwakste schakel in cybersecurity. Door gebrek aan kennis over de impact van onze acties, maken we bijna dagelijks kleine foutjes die hackers gemakkelijk kunnen uitbuiten. De grootste aandachtspunten zijn phishing, het veilig beheren van wachtwoorden, en het strikt gescheiden houden van privé- en werkgegevens in de digitale omgeving.

3 Hoe?

Leg medewerkers in eenvoudige taal uit waar ze op moeten letten en waarom dat belangrijk is. Besteed voldoende aandacht aan het waarom. Veiliger werken op je pc gaat vaak ten koste van gebruiksvriendelijkheid. Mensen zijn alleen bereid dat 'offer' te brengen als ze begrijpen wat de meerwaarde is.

2 Waarom?

Hackers richten zich zelden op specifieke slachtoffers; ze zijn opportunisten. Ze sturen hun aanvallen als hagel de wereld in, zonder te letten op wie er geraakt wordt. Hun gedachte: iemand zal wel een fout maken en in de val trappen. Als die persoon toevallig in jouw bedrijf werkt, kan hij of zij onbewust de deur voor hackers openzetten.

Meer info

Menselijke fouten blijven een groot cyberrisico, dus is bewustmaking cruciaal om veilig gedrag te stimuleren.

 [Module 2a - Standaard phishing](#)
[Module 2b - Geavanceerd phishing](#)
[Module 5b - Thuis-Werk](#)

www.unizo.be/CS4ZO-opleidingsprogramma

6. Anti-virus

Antivirussoftware is cruciaal voor de beveiliging van een bedrijf, omdat het beschermt tegen virussen, malware en andere cyberdreigingen die systemen kunnen verstoren en gegevens kunnen stelen. Het fungeert als een eerste verdedigingslinie door verdachte activiteiten te blokkeren en regelmatig te scannen. In een tijd van toenemende cyberaanvallen is het up-to-date houden van antivirussoftware een essentieel onderdeel van een sterke cybersecuritystrategie.

1 Wat?

Antivirussoftware is als basis-hygiëne voor je pc's en servers. Hoewel een antivirus alleen niet genoeg is, is een apparaat zonder antivirus een gemakkelijke prooi. Zie antivirus als het slot op je voordeur: de eerste barrière waar een hacker omheen moet zien te komen.

3 Hoe?

Het antivirussoftware pakket dat je kiest, maakt niet zoveel uit; de grote namen presteren vrijwel gelijk in vergelijkende studies. Het belangrijkste is dat je de software op alle pc's en servers installeert en deze up-to-date houdt om nieuwe bedreigingen effectief te detecteren. Idealiter combineer je antivirussoftware met een monitoringdienst, zodat professionals de meldingen van de software evalueren en je waarschuwen als er meer aan de hand is.

2 Waarom?

Hackers proberen automatisch elk apparaat dat via het internet bereikbaar is te infecteren met malware. Antivirusbedrijven volgen deze geautomatiseerde aanvallen continu en zorgen ervoor dat hun software deze bedreigingen blokkeert.

Meer info

Antivirussoftware vormt een essentiële eerste verdedigingslinie tegen malware en cyberaanvallen.

 [Module 4a - Malware](#)
[Module 4b - Ransomware](#)
[Module 6a - Beveiligingsmonitoring](#)

www.unizo.be/CS4ZO-opleidingsprogramma

Cybersecurity zonder paniek, mét plan



Bert Bleukx
Stark Security

Cybersecurity is een verhaal met vele facetten, en als ondernemer is het soms moeilijk om door de bomen het bos nog te zien. Cyberdreigingen evolueren razendsnel, in de media lezen we bijna dagelijks over nieuwe aanvallen, datalekken & miljoenen verliezen door ransomware.

De valkuil? Je laten leiden door angst of paniek. Misschien hoorde je van een getroffen concullega, of kreeg je een alarmerend bericht van een IT-leverancier. Maar angst is een slechte, en vaak dure, raadgever. Wat je nodig hebt, is geen paniecreactie, maar een cybersecuritystrategie, een plan dat in kaart brengt waar je risico's liggen en welke stappen je in welke volgorde moet zetten. Cyberveiligheid is geen einddoel, maar een voortdurend proces van inschatten, aanpassen en versterken.

Een veelvoorkomende fout bij cybersecurity is dat ondernemers denken dat ze alles in één keer moeten oplossen. Maar net zoals je een bedrijf niet in één dag bouwt, bouw je ook cybersecurity stap voor stap. Begin met het laaghangend fruit. Dit zijn maatregelen die weinig kosten en meteen impact hebben:

- Gebruik multi-factor authenticatie (MFA) op alle kritieke accounts.
- Houd software en systemen up-to-date om kwetsbaarheden te dichten.
- Zorg voor regelmatige back-ups en test of je ze vlot kunt herstellen.

- Train je medewerkers in het herkennen van phishing en andere dreigingen.
- Segmenteer je netwerk, zodat een aanval op één onderdeel niet meteen alles platlegt.

Een cybersecurityplan is echter nooit 'af'. Net zoals je bedrijfsstrategie verandert met de markt, moet je beveiliging regelmatig herbekeken en aangepast worden. Nieuwe dreigingen ontstaan, technologieën evolueren en hackers worden steeds geavanceerder. Daarom is bijsturing essentieel, een plan dat vijf jaar onaangeroerd blijft, biedt geen bescherming meer.

Een cybersecurityplan is echter nooit af. Net zoals je bedrijfsstrategie verandert met de markt, moet je beveiliging regelmatig herbekeken en aangepast worden.

De eerste stap? Informeren. Want je kunt pas actie ondernemen als je weet wat je moet doen. Deze gids is een goed begin, maar je kunt cybersecurity pas echt implementeren als je de juiste kennis hebt. Cybersecurity is geen kwestie van 'of' maar 'wanneer' je ermee aan de slag gaat. Begin vandaag, stap voor stap, en maak je onderneming sterker.

7. Toegang op afstand

Toegang op afstand biedt medewerkers de flexibiliteit om vanop eender welke locatie te werken, maar brengt ook extra cyberrisico's met zich mee. Zonder de juiste beveiligingsmaatregelen kunnen onbevoegden via die weg toegang krijgen tot gevoelige bedrijfsgegevens. Daarom is het essentieel om toegang op afstand altijd te beveiligen met sterke wachtwoorden, multi-factor authenticatie en een beveiligde verbinding, zoals een VPN. Ook regelmatige monitoring en toegangscontroles zijn cruciaal.

1 Wat?

Wanneer je vanuit huis werkt of wanneer gespecialiseerde firma's op afstand verbinding maken met jouw systemen, gebeurt dat meestal via een VPN.

Zo'n VPN moet veilig worden opgezet, omdat het een directe toegangsdeur tot je bedrijf vormt.

2 Waarom?

Alles wat aan het internet hangt, wordt gevonden door hackers. Als daar een zwakke plek in gevonden wordt, wordt dit misbruikt om binnen te breken. Een VPN hangt per definitie aan het internet. Hackers weten maar al te goed hoe veelvuldig deze technologie gebruikt wordt én hoe vaak ze onzorgvuldig wordt geconfigureerd of onderhouden.

3 Hoe?

Zorg altijd voor multi-factor authenticatie bij je VPN-verbindingen, zowel voor jou en je medewerkers bij thuiswerken als voor partners die onderhoud aan je systemen uitvoeren. Schakel VPN-verbindingen uit wanneer je ze niet nodig hebt. Als een bedrijf bijvoorbeeld één dag per maand onderhoud doet, zorg dan dat hackers de verbinding de overige 30 dagen niet kunnen misbruiken. Houd je VPN-software altijd up-to-date; security updates zijn essentieel, vooral voor toegangspunten tot je bedrijf.

Meer info

Toegang op afstand biedt flexibiliteit, maar vraagt om sterke beveiliging om misbruik en datalekken te voorkomen.

- 📄 [Module 1b - Veilig omgaan met je PC](#)
- 📄 [Module 3b - 2-Factor-Authenticatie](#)
- 📄 [Module 5c - Wifi-Cloud-VPN](#)

www.unizo.be/CS4ZO-opleidingsprogramma

Getuigenis

Broothaers NV



Broothaers B2 Mode Team

Broothaers NV is al meer dan 30 jaar een gevestigde modeagentuur. Het bedrijf verkoopt kleding aan winkels in heel België en Luxemburg en fungeert als tussenpersoon voor verschillende Europese damesmerken, voornamelijk Duitse, Scandinavische en Spaanse labels. De klanten van Broothaers bestaan uit zowel boetieks als grotere baanwinkels met meerdere filialen.

“Digitalisering zorgt voor een duidelijke tijds- en kostenbesparing. Daardoor kunnen wij ons meer focussen op persoonlijk contact met de retailers.”

Wat betekent digitalisering binnen jullie bedrijf?

Winkeliers komen bij ons de collecties bekijken, en wij geven hun bestellingen digitaal in. Die orders gaan rechtstreeks naar de fabrikanten in Duitsland, Scandinavië of andere landen. Klanten ontvangen automatisch een bevestiging met foto's, maten en bedragen in hun mailbox. Daarnaast kunnen winkeliers ook rechtstreeks uit onze stock bestellen via een B2B-platform met een persoonlijke login. Dat is een enorm verschil met vroeger, toen bestellingen nog telefonisch binnenkwamen en alles manueel moest worden doorgegeven. Nu verloopt alles sneller, eenvoudiger en met veel minder werk.

Wat is de belangrijkste reden om te digitaliseren?

Digitalisering zorgt voor een duidelijke tijds- en kostenbesparing, onder andere op het vlak van personeel. Daardoor

kunnen wij ons meer focussen op persoonlijk contact met de winkels. Daarnaast kunnen we via digitale tools ook meteen zien hoe hun verkoop verloopt. Zo kunnen we sneller inspelen op items die minder goed verkopen en die omruilen voor beter scorende stuks.

Is jullie onderneming reeds actief in de cloud?

Ja, onze volledige werking is gecentraliseerd in de cloud. Dat technische luik wordt beheerd door onze IT-partner DVIT, die ons ondersteunt en snel ingrijpt bij vragen of problemen.

Wat is de belangrijkste reden om in de cloud te werken?

Omdat we heel vaak onderweg zijn, in België én in het buitenland, is het handig dat we overal toegang hebben tot onze gegevens. Met een laptop of tablet kunnen we bij klanten meteen alles raadplegen. Dat maakt ons werk veel flexibeler en efficiënter.



Nathalie Broothaers
Broothaers NV

Ga voor een strategische compagnon de route!



Wat is het belang van een IT partner voor jullie onderneming?

IT is een complexe wereld, en wij zijn daar niet in thuis. Daarom is een betrouwbare IT-partner voor ons onmisbaar. Wanneer er zich een probleem voordoet, bijvoorbeeld tijdens het opnemen van bestellingen, is het cruciaal dat we iemand kunnen bellen die snel helpt. DVIT is altijd bereikbaar en lost technische issues onmiddellijk op, wat voor ons enorm belangrijk is.

Wat is de impact van een IT-partner op jullie bedrijf?

De samenwerking met DVIT verloopt optimaal. Ze zijn snel, bereikbaar en nemen heel wat werk uit handen. Dankzij hun expertise kunnen wij ons focussen op wat voor ons telt: het contact met onze klanten.

Welke rol moet een IT-partner opnemen?

DVIT is zowel proactief als adviserend. Ze informeren ons regelmatig, denken

mee wanneer we vastlopen en geven advies over nieuwe technologieën. We kunnen altijd bij hen terecht voor uitleg of ondersteuning.

Wie is DVIT?

DVIT is een IT-bedrijf uit Erpe-Mere dat bedrijven volledig ontzorgt op vlak van ICT. Van netwerk tot security, van cloud tot support, DVIT zorgt ervoor dat alles gewoon werkt. Sinds 2022 maakt DVIT deel uit van de AXI Group, waardoor we extra slagkracht, expertise en schaalbare technologie-oplossingen kunnen aanbieden.

Hoe verloopt de samenwerking tussen DVIT en Broothaers?

David Van Impe: We werken al zo'n 14 à 15 jaar samen. Broothaers is altijd snel mee geweest in onze aanbevelingen. Omdat ze vaak onderweg zijn, was het voor hen essentieel om een systeem te hebben dat overal bereikbaar is.

We hebben hen vroegtijdig naar de cloud gemigreerd en werken vandaag

met de KMO in de Cloud-oplossing van ClearMedia. Zo kunnen ze wereldwijd veilig en eenvoudig inloggen op hun applicaties: Microsoft Office, e-mail en de aankoopportalen van hun modemerken, meestal in Duitsland. Daarnaast beheren wij hun randapparatuur, domeinnamen, beveiliging en website. Kortom: het volledige IT-plaatje.

Welke maatregelen hebben jullie al genomen rond cybersecurity?

We zijn ons zeer bewust van het belang van cybersecurity. Onze medewerkers gebruiken tweestapsverificatie wanneer nodig, en we worden regelmatig geïnformeerd en begeleid door DVIT om veilig te blijven werken.

AI, we kunnen er niet omheen. Hebben jullie hier al stappen ondernomen?

We komen steeds vaker in aanraking met AI. Zo zagen we twee jaar geleden een modeshow waarbij alle modellen volledig door AI waren gegenereerd, iets waar ik persoonlijk geen voorstander van ben, want echte mannequins blijven toch mooier.

Daarnaast gebruiken we ChatGPT steeds meer als hulpmiddel in dagelijkse taken zoals mails, teksten en andere communicatie.

Is er een duidelijke roadmap voor de implementatie van AI?

We zitten momenteel nog in de experimenteerfase met ChatGPT. Het interesseert me wel en ik wil er in de toekomst zeker meer over leren en meer mee doen. Maar voorlopig ontdekken we vooral wat mogelijk is.

Hoe zien jullie de toekomst van Broothaers en de impact van digitalisering?

Digitalisering zal alleen maar belangrijker worden. In sommige landen worden collecties nu al volledig digitaal besteld, zonder dat klanten nog persoonlijk langskomen.

In België blijft persoonlijk contact voorlopig belangrijker, maar binnen 5 tot 10 jaar verwacht ik dat ook onze sector op dat vlak verder zal digitaliseren. De evolutie gaat snel, en onze branche zal daarin moeten volgen.

“De digitale evolutie gaat snel, en onze branche zal daarin moeten volgen.”

Nathalie Broothaers, Broothaers NV



Expert aan het woord

ClearMedia



Dustin Benner
ClearMedia

ClearMedia

Als zelfstandige of kleine ondernemer ben je voortdurend bezig met je klanten, je dienstverlening en het draaiende houden van je zaak. Cybersecurity staat dan vaak niet bovenaan je prioriteitenlijst. Toch wordt **élke ondernemer, groot of klein, steeds afhankelijker van digitale technologieën en online systemen. En daarmee groeit ook het risico op cyberaanvallen.**

In tegenstelling tot grote bedrijven met een gespecialiseerde IT-afdeling, sta je als zelfstandige, micro- of kleine onderneming vaak alleen voor de beveiliging van je bedrijf. Hackers weten dat en richten zich bewust op dat type van ondernemingen, omdat die meestal

minder beveiligingsmaatregelen hebben. Een cyberaanval kan niet alleen leiden tot verlies van waardevolle gegevens, maar ook je bedrijfsvoering stilleggen. Zonder toegang tot je klantgegevens, facturatie of boekhoudsoftware sta je met de rug tegen de muur.

Cyberveiligheid hoeft niet complex of duur te zijn

De grootste cyberrisico's voor kleine ondernemingen

Je hoeft geen IT-expert te zijn om je risico's te begrijpen. De meest voorkomende dreigingen zijn:

- Phishing: Valse e-mails die je proberen te misleiden om op een link te klikken of inloggegevens door te geven.
- Ransomware: Kwaadaardige software die je bestanden versleutelt en pas vrijgeeft na betaling van losgeld.
- Datalekken: Het verlies van klantgegevens door een hack of menselijke fout kan juridische en financiële gevolgen hebben.

Wat kun je zelf doen?

Cyberveiligheid hoeft niet complex of duur te zijn. Een paar eenvoudige maatregelen maken al een wereld van verschil:

- Gebruik sterke wachtwoorden en activeer multi-factor authenticatie (MFA) op je e-mails en bedrijfssoftware.
- Werk je software en toestellen regelmatig bij zodat beveiligingslekken gedicht worden.
- Wees alert op verdachte e-mails en train jezelf en eventuele medewerkers in het herkennen van cyberdreigingen.
- Maak back-ups van je belangrijkste gegevens en bewaar die op een aparte locatie.
- Gebruik een betrouwbare antivirus- en firewalloplossing om malware te blokkeren.

Meer dan technologie: bewustwording en wetgeving

Cybersecurity draait niet alleen om technologie. Het gaat ook om bewuste keuzes maken en veilig online gedrag. Als zelfstandige ben jij zélf de eerste verdedigingslinie. Dat betekent bijvoorbeeld dat je niet zomaar software moet installeren van onbekende bronnen of je bedrijfs wachtwoorden niet op een post-it naast je computer moet bewaren. Daarnaast verplicht de wetgeving je om zorgvuldig met persoonsgegevens om te gaan. De Algemene Verordening Gegevensbescherming (AVG) eist dat je klantgegevens correct bewaart en beveiligt.

Begin vandaag, stap voor stap

Je hoeft niet alles tegelijk te doen. Start met kleine, haalbare stappen die direct effect hebben. Door bewust met cybersecurity om te gaan, bescherm je niet alleen je onderneming, maar ook je klanten en leveranciers.

Wil je meer weten?

Bekijk dan de [UNIZO-videolessen](#) over cybersecurity en ontdek hoe je je zaak beter kunt beveiligen zonder onnodige kosten of complexe IT-oplossingen.



8. Wargame

Een wargame of simulatie is een onmisbaar onderdeel van een doordachte cybersecuritystrategie. Door een denkbeeldige cyberaanval stap voor stap te doorlopen, ontdek je waar de zwakke plekken zitten in je organisatie en hoe goed je team is voorbereid op een echte crisissituatie. Zo'n oefening maakt risico's tastbaar, verhoogt het bewustzijn bij medewerkers en helpt je om sneller, gericht en doeltreffender te reageren als het écht misgaat.

1 Wat?

Zie het als een brandoefening, maar dan voor je digitale wereld. Wat als... Simuleer een hackingaanval op papier en beoordeel hoe goed je bent voorbereid om zo'n aanval te weerstaan. Ga ervan uit dat het al gebeurd is, wat doe je dan?

2 Waarom?

Als je slachtoffer wordt van een hack, is paniek een slechte raadgever. Door van tevoren te oefenen op zulke situaties, kun je veel beter en effectiever beslissingen nemen. Goede communicatie is cruciaal tijdens een aanval; door hier vooraf over na te denken, zorg je ervoor dat je communicatie veel beter verloopt dan wanneer je het op het moment zelf moet improviseren.

3 Hoe?

Overleg met belangrijke personen over mogelijke aanvallen: wat zou echt schadelijk zijn als het gebeurt? Simuleer vervolgens een scenario waarin dit al is gebeurd en bedenk acties om de schade te beperken. Je hebt ICT nodig om alles te herstellen, maar dat kost tijd. De vraag is: hoe overbrug je die tijd? Wat vertel je aan klanten en leveranciers, en hoe kun je ondanks de hack je bedrijfsactiviteiten voortzetten?

Meer info

Een simulatie van een cyberaanval helpt je inschatten hoe goed je bent voorbereid op een echte digitale crisis.

 [Module 4a - Malware](#)
[Module 4b - Ransomware](#)
[Module 6a - Beveiligingsmonitoring](#)

www.unizo.be/CS4ZO-opleidingsprogramma

Cyberveiligheid: is het nodig voor jouw onderneming?

Cybercriminaliteit stopt niet bij grote bedrijven. Ook zelfstandigen en kleine ondernemingen zijn een doelwit, vaak omdat hun beveiliging minder sterk is. Een cyberaanval kan ernstige gevolgen hebben: van gestolen klantgegevens tot een vergrendeld facturatiesysteem waardoor je je werk niet meer kunt doen. Een cyberverzekering kan helpen om de financiële schade te beperken, maar is het ook een slimme investering voor jouw onderneming?

Waarom zou je een cyberverzekering overwegen?

Je auto, brandverzekering en beroepsaansprakelijkheid heb je waarschijnlijk goed geregeld. Maar als je bedrijf afhankelijk is van digitale systemen, en dat is bij de meeste ondernemers het geval, is de vraag: wat gebeurt er als een cyberaanval je bedrijf platlegt?

Een cyberverzekering helpt je om:

- De kosten van een cyberaanval op te vangen: Denk aan IT-forensisch onderzoek, herstel van systemen en juridische bijstand.
- Je bedrijf draaiende te houden: Als je bedrijf tijdelijk offline moet, kan een verzekering inkomstenverlies (gedeeltelijk) dekken.
- Schadeclaims door klanten te vermijden: Als klantgegevens uitlekken, kan een verzekering helpen bij schadevergoeding en juridische kosten.
- Hulp te krijgen van specialisten: Veel verzekeraars bieden crisismanagement aan, zodat je snel de juiste experts inschakelt.

Wat dekt een cyberverzekering?

Niet elke cyberverzekering is hetzelfde, maar in de meeste gevallen bieden ze dekking voor:

Herstelkosten: IT-experts die systemen herstellen en data terughalen.

Bedrijfsschade: Inkomstenverlies door downtime na een aanval.

Wettelijke kosten: Boetes en claims bij datalekken of overtreding van de AVG. Onderhandeling bij ransomware: Begeleiding en hulp bij afpersing na een aanval.

Let op: sommige basispolissen dekken enkel IT-herstel, terwijl uitgebreidere polissen ook reputatieschade en juridische kosten vergoeden.

Hoe kies je de juiste cyberverzekering?

- **Evalueer je risico's:** Hoe afhankelijk ben je van digitale systemen? Heb je klantgegevens in beheer? Een webshop? Cloudsoftware?
- **Vergelijk polissen:** Niet elke verzekering dekt ransomware of datalekken op dezelfde manier. Kijk naar de kleine lettertjes.
- **Let op de voorwaarden:** Sommige verzekeringen eisen dat je basismaatregelen neemt, zoals een firewall en back-ups.
- **Kijk of je al verzekerd bent:** Soms biedt je bestaande verzekering al een basis cyberdekking.

Wil je meer informatie over de mogelijkheden om je te verzekeren tegen cyberincidenten? Klik [hier](#)

NIS2-richtlijn, wat betekent dit voor mijn onderneming?

Misschien heb je al gehoord van de NIS2-richtlijn, een nieuwe Europese wetgeving die bedrijven verplicht om striktere cybersecuritymaatregelen te nemen.

Voor veel zelfstandigen en kleine ondernemingen is NIS2 niet direct van toepassing, maar de impact op je keten en klanten is wél belangrijk.

De nieuwe regels richten zich op bedrijven die als kritiek of essentieel worden beschouwd voor de economie, zoals telecom, energie, transport, financiële instellingen en leveranciers van digitale diensten. Zij moeten hun cyberbeveiliging aanzienlijk versterken en rapporteren over incidenten. Maar wat betekent dat voor jou als kleinere onderneming?

Waarom NIS2 ook voor jou relevant is

- Jouw klanten en partners kunnen jou als zwakke schakel zien. Grotere bedrijven zullen striktere cybersecurity-eisen stellen aan hun leveranciers en dienstverleners, inclusief KMO's en zelfstandigen.
- Sterkere cybersecurity wordt een vereiste om mee te blijven spelen. Wil je blijven samenwerken met grotere klanten of overheden? Dan moet je misschien aantonen dat je basisbeveiliging op orde is.
- Een cyberaanval bij jou kan je hele supply chain raken. Zelfs als jij geen verplichtingen hebt onder NIS2, kan een hack in jouw onderneming gevolgen hebben voor andere bedrijven waarmee je samenwerkt.

Wat kun je doen?

- Je hoeft niet meteen een volledig NIS2-compliant bedrijf te worden, maar je kunt wel zorgen dat je onderneming niet de zwakste schakel wordt.
- Begin met:
- Sterke wachtwoorden en multi-factor authenticatie instellen op je belangrijkste accounts.
- Software up-to-date houden om beveiligingslekken te dichten.
- Back-ups maken en ze offline bewaren, zodat je snel kunt herstellen bij een aanval.
- Veilig omgaan met klantgegevens, want ook de AVG (GDPR) stelt hier regels voor.
- Je bewust worden van phishing en social engineering-aanvallen, zodat je niet per ongeluk de deur openzet voor cybercriminelen.

Cybersecurity wordt een concurrentievoordeel. Bedrijven die hun basisbeveiliging op orde hebben, kunnen aantonen dat ze een betrouwbare partner zijn.

Wil je weten of NIS2 voor jouw sector verplicht is? Bezoek de website van [Safe-on-web@work](#) en check de Belgische regels.

Safeonweb@work

Safeonweb@work is een initiatief van het Centrum voor Cybersecurity België (CCB) voor Belgische organisaties en ondernemingen. Het doel is de cyberveiligheid van de Belgische ondernemingen en organisaties te versterken door hen via verschillende diensten advies, aanbevelingen en instrumenten te verstrekken waarmee ze de kwetsbaarheden van hun systemen kunnen identificeren en verzachten en worden gewaarschuwd over cyberbedreigingen.

7 Stappenplan

Maak jouw organisatie klaar voor de NIS2-richtlijn met onze zeven cruciale stappen. Van het in kaart brengen van kwetsbaarheden tot het opleiden van je medewerkers, deze praktische stappen helpen je om je IT-beveiliging te versterken en aan alle vereisten te voldoen.

- 1 Heeft NIS2 op mij betrekking?
- 2 Registreer jouw NIS2-entiteit zo snel mogelijk
- 3 Meld significante incidenten
- 4 Voer een strategische risicobeoordeling uit
- 5 Plan cyberbeveiligingstraining
- 6 De beveiligingsmaatregelen implementeren
- 7 De beveiligingsmaatregelen controleren

Wil je meer weten?

Raadpleeg de aanbeveling van het Centrum voor Cybersecurity België (CCB) om in 7 stappen te voldoen aan de Belgische NIS2-wetgeving.



Conclusie

De mode-industrie draait al lang niet meer enkel om creatie en productie: ook de digitale keten bepaalt vandaag het succes. Bestellingen van retailers verlopen via online B2B-platformen, productie- en voorraadplanning worden digitaal aangestuurd en leveranciers, ateliers en distributiepartners wisselen continu data uit. IT is daarvoor niet langer ondersteunend, maar een cruciale pijler van de werking.

Cybersecurity als bouwproject, geen eindpunt

Cyberveiligheid hoeft geen ingewikkeld verhaal te zijn. Deze gids reikt duidelijke bouwstenen aan die elk bedrijf kan toepassen: van het inventariseren van je systemen en het updaten van software, tot het implementeren van multi-factor authenticatie, netwerkwisdom en gebruikersbewustzijn. Ook tools zoals antivirussoftware, Mobile Device Management en een incident responseplan dragen bij aan een solide digitale basis.

NIS2 en ketenverantwoordelijkheid

Met de komst van de Europese NIS2-richtlijn wordt duidelijk dat cybersecurity niet langer vrijblijvend is. Zelfs als jouw onderneming niet rechtstreeks onder de wet valt, zullen grotere klanten, locaties of partners strengere eisen stellen aan leveranciers. Cyberveiligheid wordt daarmee niet alleen een noodzaak, maar ook een concurrentievoordeel. Bedrijven die kunnen aantonen dat hun basisbeveiliging op orde is, versterken hun positie binnen de waardeketen.

Cyberverzekering als vangnet

Een cyberverzekering kan geen incidenten voorkomen, maar wel helpen om de schade te beperken. Van IT-forensisch onderzoek en juridische ondersteuning tot inkomensverlies en reputatieschade: wie voorbereid wil zijn op het ergste, doet er goed aan om ook dit aspect mee te nemen in zijn digitale strategie.

De rol van de IT-partner

Geen enkel bedrijf hoeft deze weg alleen te bewandelen. Een goede IT-partner is meer dan technische ondersteuning, het is een strategische meedenker. Of het nu gaat om cloudmigraties, cybersecuritymaatregelen of proactieve monitoring: wie kiest voor de juiste partner, bouwt aan continuïteit, efficiëntie en gemoedsrust.

Actie, stap voor stap

Digitale weerbaarheid hoeft niet in één dag opgebouwd te worden. Begin met laagdrempelige maatregelen, zoals wachtwoordbeheer of software-updates. Bereid stap voor stap uit met gebruikersopleidingen, simulatieoefeningen (wargames) en duidelijke afspraken met partners en leveranciers. Gebruik deze gids als een praktisch kompas, niet als een theoretisch rapport.

Cyberveiligheid is geen doel op zich, maar een voorwaarde om te blijven groeien, samenwerken en leveren in een digitale economie. Zet vandaag de eerste stap, zodat je morgen met vertrouwen kan blijven ondernemen.

Heb je vragen of nood aan ondersteuning bij de eerste stappen?



Contacteer de UNIZO Ondernemerslijn voor advies op maat van jouw onderneming of bezoek www.unizo.be/digitale-safety-first voor meer tools, tips en opleidingen.

+32 2 212 26 78
ondernemerslijn@unizo.be



